المحكمة الرقمية والجريمة المعلوماتية

دراسة مقارنة



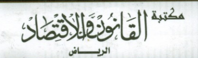
المستشار القانوني

عبد الصبور عبد القوي على مصري

ماجستير في القانون العام والقانون الطبي

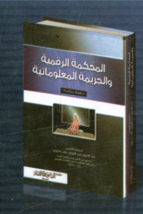
عضو الهيئة الإسلامية العالمية للاقتصاد والتمويل

باحث دكتوراه



مكتبة القانون والاقتصاد

الرياض



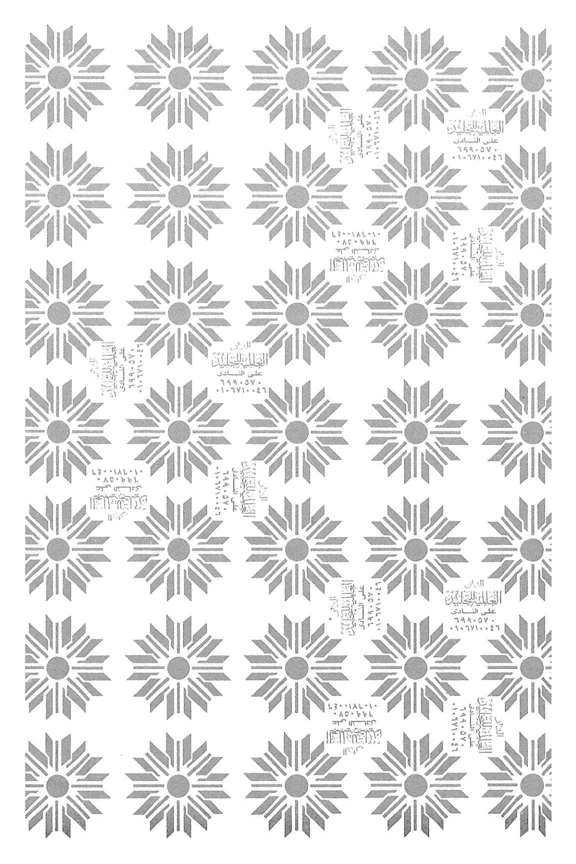


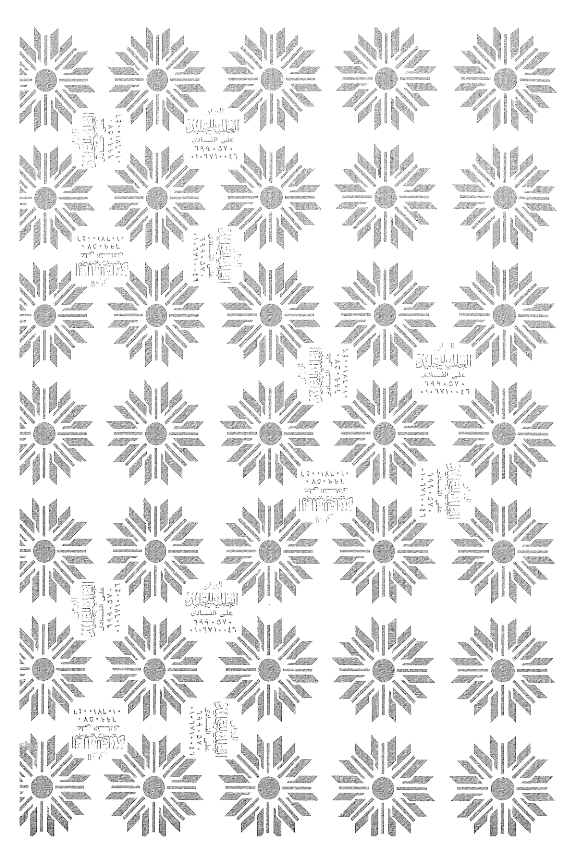



ISBN 978-603-8106-04-4
9 786038 106044 >

Designed by : www.elchimy.com




الدار
العالمية للتجليد
على النـادى
٦٩٩٠٥٧٠
٠١٠٦٧١٠٠٤٦





المحكمة الرقمية

والجريمة المعلوماتية



المحكمة الرقمية والجريمة المعلوماتية

دراسة مقارنة

المستشار القانوني

عبد الصبور عبد القوي علي مصري

ماجستير في القانون العام والقانون الطبي

عضو الهيئة الإسلامية العالمية للاقتصاد والتمويل

باحث دكتوراه

الطبعة الأولى

1433 هـ/2012 م



ح مكتبة القانون والاقتصاد، 1433 هـ

فهرسة مكتبة الملك فهد الوطنية أثناء النشر

مصري، عبد الصبور عبدالقوي علي

المحكمة الرقمية والجريمة المعلوماتية دراسة مقارنة./ عبد الصبور عبدالقوي علي مصري - الرياض، 1433 هـ

..ص ؛ ..سم

ردمك: 978-603-8106-04-4

1 - أمن المعلومات 2- الحواسيب - قوانين وتشريعات 3- جرائم الحواسيب أ. العنوان

ديوي 344.0999 1433/1138

رقم الإيداع: 1433/1138

ردمك: 978-603-8106-04-4

الطبعة الأولى

1433 هـ/2012 م

ISBN 978-603-8106-04-4

9 786038 106044 >

مكتبة القانون والاقتصاد الرياض

المملكة العربية السعودية - الرياض - العليا - ص.ب 9996 - الرياض 11423

هاتف: 4623956 - 2791158 - فاكس: 2791154 - جوال: 0505269008

www.yafoz.com.sa

info@yafoz.com.sa

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

﴿وَمَن يَتَّقِ اللَّهَ يَجْعَل لَّهُ مِنْ أَمْرِهِ يُسْرًا (4) ذَلِكَ أَمْرُ اللَّهِ أَنزَلَهُ إِلَيْكُمْ وَمَن يَتَّقِ اللَّهَ يُكَفِّرْ عَنْهُ سَيِّئَاتِهِ وَيُعْظِمْ لَهُ أَجْرًا (5)﴾

سورة الطلاق



يقول أحد الكتاب[1]:

« إني رأيت أنه لا يكتب إنسان كتاباً في يومه

إلا قال في غده: لو غيِّر هذا لكان أحسن،

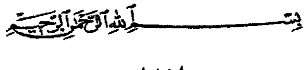
ولو زيد كذا لكان يُستحسن ولو قدّم هذا لكان أفضل،

ولو ترك هذا لكان أجمل،

وهذا من أعظم العبر هو دليل على استيلاء النقص على جملة البشر»

(1) العماد الأصفهاني، رحمه الله.





إهداء

إلى روح «الأبان» اللذان تعبا لأجلنا والمدرسة التي تخرجنا منها متعلمان القيم والمباديء والأخلاق التي لا تتجزء ولا تموت، نسأل الله أن يتغمدهما برحمته وأن يسكنهما فسيح جناته.

إلى «الوالدتان» روحنا وحياتنا وأملنا وعملنا وبسمة مستقبلنا المشرق.

إلى كل من تعثَّرت به السبل وضاع منه الطريق وأظلمت عليه الدنيا افتح عيناك ترى وهج الشمس نهاراً وضوء القمر ليلاً يبعث فيك الأمل وحب الحياة.

عبد الصبور عبد القوي علي المصري



مقدمة

إن التطورات الحديثة في تقنية المعلومات أحدثت تغيُّرات مستمرة ومضطردة في أساليب العمل والميادين كافة إذ أصبحت عملية انتقال المعلومات عبر الشبكات المحلية والدولية وأجهزة الحاسب من الأمور الروتينية في عصرنا الحالي وإحدى علامات العصر المميزة التي لا يمكن الاستغناء عنها لتأثيرها الواضح في تسهيل متطلّبات الحياة العصرية من خلال تقليل حجم الأعمال وتطوير أساليب توفير المعلومات ؛حيثُ أن انتشار أنظمة المعلومات الإلكترونية أدَّت إلى أن تكون عرضة للاختراق ؛لذلك أصبحت هذه التقنية سلاحاً ذو حدين تحرص المنظمات على اقتناءه وتوفير سبل الحماية له.

وأصبح موضوع الأمن المعلوماتي يرتبط ارتباطاً وثيقاً بأمن الحاسبات فلا يوجد أمن للمعلومات إذا لم يراعَ أمن الحاسبات، وفي ظل التطورات المتسارعة في العالم والتي أثّرت على الإمكانات التقنية المتقدمة المتاحة والرامية إلى اختراق منظومات الحاسب بهدف السرقة ،أو تخريب المعلومات والبيانات ،أو تدمير أجهزة الحاسب، كان لا بد من التفكير الجدي لتحديد الإجراءات الدفاعية والوقائية وحسب الإمكانات المتوفرة لحمايتها من أي اختراق أو تخريب، وكان على إدارة المنظمات أن تتحمَّل مسئولية ضمان خلق أجواء أمنية للمعلومات تضمن الحفاظ عليها.

وجاءت فكرة المحكمة الرقمية نتيجة لانتقالنا من الإجرام العادي

والجرائم التقليدية إلى الإجرام الرقمي والجرائم المعلوماتية، وكان لابد من إنشاء محكمة متخصصة للجرائم التي ترتكب عبر الانترنت وما أطلق عليه الغالبية العظمى من الفقهاء مسمًّى «المحكمة الرقمية»، وهي المحكمة التي تختص بالنظر في الجرائم التي تُرتَكب عبر الوسائط الإليكترونية باختلاف مسميات تلك الوسائط، والمجرم الذي يقع تحت طائلة العقاب أطلقت عليه «المجرم الإلكتروني»، فالمجرم الإلكتروني يختلف باختلاف ارتكابه للجريمة فيقسَّم إلى عدَّة أشخاص كما سنوضحها في صدر هذا المؤلَّف ودوافعهم الإجرامي لارتكاب تلك الجرائم.

أما القاضي، فهو القاضي الرقمي فهو شخص متخصص في النظر في الجرائم التي تُرتَكب عبر الانترنت ومُلم بالقواعد الوارد في الأنظمة وقوانين مكافحة الجرائم المعلوماتية والقوانين التي تحكم استخدام الانترنت سواء كان النزاع مدنياً أو جنائياً أو تجارياً بمعنى اختلاف نوع الدعوى سواء مدنية أو جنائية أو تجارية.

وأما عن الأنظمة والقوانين محل العقوبة بالمجرم الإليكتروني، فهي تلك العقوبات الواردة في الأنظمة والقوانين التي تحكم استخدام الانترنت أو الوسائط المعلوماتية.

لذلك كان لزاماً علينا ألا نخلط بين مسمًّى المحكمة الرقمية والمحكمة الإليكترونية، وإن كنت أجد أن هناك فارق بينهما فالمحكمة الرقمية هي المحكمة التي تختص بالنظر في الدعاوى والجرائم التي تُرتَكب عبر الانترنت وتتكوَّن من قاضٍ متخصص ومحامٍ متخصص في تلك الدعوى والجرائم. أما المحكمة الإلكترونية فهي المحكمة التي تستخدم أساليب التكنولوجيا الحديثة في سير عملها ونظر القضايا والدعوى كعرض القضايا على شاشات إلكترونية أو استخدام الكتابة الإليكترونية بين أطراف الدعوى وغيرها من وسائل استخدام التكنولوجيا الحديثة.

فيختلف القانون الواجب التطبيق على الدعاوى والقضايا التي تنظر

في المحاكم الرقمية باختلاف البلاد التي تُطبَّق فيه المهم، أن المحكمة الرقمية محكمة مختصة بدعاوى بسوف نتولى تفصيلها، وكذلك سوف نتناول إجراءات التحقيق والقبض والتفتيش والإثبات في تلك الجرائم وما يدور عن جزئيات هذا الموضوع من تساؤلات أجدها مهمة في هذا العصر الذي سيطر استخدام الانترنت فيه على شتى مناحي الحياة.

وكما نعرف تُعتبر السويد أول دولة تسن تشريعات خاصة بجرائم الحاسب الآلي والانترنت؛ حيث صدر قانون البيانات السويدي عام (1973م) الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي إضافة إلى شموله فقرات عامة تشمل جرائم الدخول غير المشروع على البيانات الحاسبية، أو تزويرها، أو تحويلها، أو الحصول غير المشرع عليها رغم ذلك لا ننسى حادث اختراق موقع وزارة الدفاع الأمريكية.

وتلت الولايات المتحدة الأمريكية السويد حيث شرّعت قانوناً خاصاًبحماية أنظمة الحاسب الآلي (1976م – 1985م)، وفي عام (1985م) حدّد معهد العدالة القومي خمسة أنواع رئيسة للجرائم المعلوماتية وهي: جرائم الحاسب الآلي الداخلية، جرائم الاستخدام غير المشروع عن بعد، جرائم التلاعب بالحاسب الآلي، دعم التعاملات الإجرامية، وسرقة البرامج الجاهزة والمكونات المادية للحاسب. وفي عام (1986م) صدر قانوناً تشريعاً يحمل الرقم (1213) عرّف فيه جميع المصطلحات الضرورية لتطبيق القانون على الجرائم المعلوماتية كما وضعت المتطلبات الدستورية اللازمة لتطبيقه، وعلى أثر ذلك قامت الولايات الداخلية بإصدار تشريعاتها الخاصة بها للتعامل مع هذه الجرائم ومن ذلك قانون ولاية تكساس لجرائم الحاسب الآلي.

وتأتي بريطانيا كثالث دولة تسن قوانين خاصة بجرائم الحاسب الآلي حيث أقرّت قانون مكافحة التزوير والتزييف عام (1981م) الذي شمل في تعاريفه الخاصة بتعريف أداة التزوير وسائط التخزين الحاسبية المتنوعة أو أي أداة أخرى يتم التسجيل عليها سواء بالطرق التقليدية أو الإليكترونية

أو بأي طريقة أخرى. وتُطبِّق كندا قوانين متخصصة ومفصلة للتعامل مع جرائم الحاسب الآلي والانترنت؛ حيث عدلت في عام (1985م) قانونها الجنائي بحيث شمل قوانين خاصة بجرائم الحاسب الآلي والانترنت، كما شمل القانون الجديد تحديد عقوبات المخالفات الحاسبية، وجرائم التدمير، أو الدخول غير المشروع لأنظمة الحاسب الآلي.

وسنّت الدنمارك في عام (1985م) أول قوانينها الخاصة بجرائم الحاسب الآلي والانترنت والتي شملت في فقراتها العقوبات المحددة لجرائم الحاسب الآلي كالدخول غير المشروع إلى الحاسب الآلي، أو التزوير، أو أي كسب غير مشروع سواء للجاني، أو لطرف ثالث، أو التلاعب غير المشروع ببيانات الحاسب الآلي كإتلافها أو تغييرها أو الاستفادة منها. وكانت فرنسا من الدول التي اهتمت بتطوير قوانينها الجنائية للتوافق مع المستجدات الإجرامية حيث أصدرت في عام (1988م) القانون رقم (19-88)[1] الذي أضاف إلى قانون العقوبات الجنائي جرائم الحاسب الآلي والعقوبات المقررة لها. أما في هولندا فلقاضي التحقيق الحق بإصدار أمره بالتصنُّت على شبكات الحاسب الآلي متى ما كانت هناك جريمة خطيرة، كما يُجيز القانون الفنلندي لمأمور الضبط القضائي حق التصنُّت على المكالمات الخاصة بشبكات الحاسب الآلي، كما تعطي القوانين الألمانية الحق للقاضي بإصدار أمره بمراقبة اتصالات الحاسب الآلي وتسجيلها والتعامل معها وذلك خلال مدة أقصاها ثلاثة أيام. وفي اليابان قوانين خاصة بجرائم الحاسب الآلي والانترنت، ونصت تلك القوانين على أنه لا يلزم مالك الحاسب الآلي المستخدم في جريمة ما التعاون مع جهات التحقيق أو إفشاء كلمات السر التي يستخدمها إذا ما كان ذلك سيؤدي إلى إدانته. كما يوجد في المجر و بولندا، قوانين خاصة بجرائم الحاسب الآلي والانترنت تُوضِّح كيفية التعامل مع تلك الجرائم ومع المتهمين فيها، وتعطي تلك القوانين المتهم الحق في عدم طبع سجلات الحاسب الآلي

---

(1) Computer Criminals by Laura E. Quarantiello, Tiare Publications, 1996.

أو إفشاء كلمات السر، أو الأكواد الخاصة بالبرامج. وعلى مستوى الدول العربية، ففي مصر مثلاً لا يوجد نظام قانوني خاص بجرائم المعلومات.

اهتمّت جل الدول العربية بهذا الموضوع خلال الفترة الممتدة ما بين 2000 و2009م، ومن النادر اليوم أن نجد خلو تشريع هذه الدول من قوانين تنظم التجارة الإلكترونية والتوقيع الإلكتروني. ولو شئنا سوق الأمثلة لتزاحمت أمامنا النماذج بما يفيض عن غرض هذه الورقة، ولغطت هذه الأمثلة كل دول المغرب العربي، والخليج العربي، والدول الأخرى. وهكذا ففي مملكة البحرين صدر قانون التجارة الإلكترونية بتاريخ: 14 سبتمبر 2002 م، كما صدر في الأردن القانون رقم 85 لسنة 2001 م، قانون المعاملات الإليكتروني. وفي تونس صدر القانون عدد 83 لسنة 2000 م الخاص بالمبادلات الإليكترونية. ويسري نفس الشيء على المغرب، والجزائر وتونس وليبيا ولبنان والإمارات العربية المتحدة... الخ. فإذا كان استخدام الانترنت في الأغراض التجارية بدأ في الانتشار على الصعيد العالمي منذ 1992 م، فصار كمروج للسلع والخدمات. وبدأ رجال الأعمال وأصحاب المؤسسات والشركات التجارية في الإقبال على المواقع الخاصة بهذا الغرض، وأصبحوا يبرمون الصفقات عن طريق مراسلاتهم عبر البريد الإلكتروني، كما صاروا يعرضون منتجاتهم وخدماتهم من خلال مواقع لهم على شبكة الانترنت. وصدرت قوانين عربية تخص الجريمة المعلوماتية مثل القانون السوداني سنة 2006 م، وكذلك قانون الإمارات العربية المتحدة، أي القانون الاتحادي رقم 2 لسنة 2006 م في شأن مكافحة جرائم تقنية المعلومات. ونظام المملكة العربية السعودية المتعلق: بمكافحة جرائم المعلوماتية، الصادر بالمرسوم الملكي رقم: 17 بتاريخ 1428/3/8.

ولو نظرنا إلى مصر فإن القانون المصري يجتهد بتطبيق قواعد القانون الجنائي التقليدي على الجرائم المعلوماتية والتي تفرض نوعاً من الحماية الجنائية ضد الأفعال الشبيهة بالأفعال المكوِّنة لأركان الجريمة المعلوماتية. وكذا الحال بالنسبة لمملكة البحرين فلا توجد قوانين خاصة بجرائم

الانترنت، وإن وجد نص قريب من الفعل المرتَكب فإن العقوبة المنصوص عليها لا تتلاءم وحجم الأضـرار المترتِّبة على جريمة الانترنت. فالجريمة مرتبطة بالإنسان وجوداً وعدماً والإنسان مرتبط بالمجتمع، وكما أن الصلة وطيدة بين الجريمة والمجتمع، فإن القرابة وطيدة بين تطوُّر المجتمع الحضاري والعلمي والتكنولوجي والجريمة، وقد تكون تلك الصلة بين الجريمة والتطور مثيرة للدهشة ولكن سرعان ما تكشف هذه الدهشة ستارها عندما نعلم أن تطوُّر المجتمع وما يُصاحبه من تطوُّر علمي وتكنولوجي ينعكس أثـره على تطوُّر الجريمة، فالجريمة باعتبارها إحدى صور إفرازات المجتمع يصلها ما يصل المجتمع من تطوُّر، ومرجع ذلك أن مُرتكِب الجريمة وضحيتها عضوان في المجتمع ويتأثران بحياته وثقافته وتطوُّره وما يصل إليه المجرم من براعة ودراية نتيجة لهذه الثقافة والتعليم يحاول استخدامها في جريمته فالجريمة محصِّلة كل ذلك.

لقد أصبحت المعلومة هي السلعة الرئيسة في العالم، فكل الدول أصبحت لا تُقاس بقوتها العسكرية، أو قواتها، أو ثروتها، ولكن سيكون المقياس الأول لقوة الدولة هي مقدار ما تُنتجه من معلومات ومن صناعة المعلومات واستخدامها والتعامل معها، فالمعلومة قوة فهذا الانفجار المعلوماتي الذي نشهده الآن هو ثمرة المزج بين تكنولوجيا الاتصالات وتكنولوجيا الحاسب الآلي أدَّى إلى ميلاد علم جديد هو علم telematique وهو مصطلح مركب من المقطع الأول لكلمة اتصال عن بعد tele communication والمقطع الثاني من كلمة المعلوماتية informatique وهو يعنى بذلك علم الاتصال المعلوماتي عن بعد أو من مسافة، وبذلك تنتقل الحضارة الإنسانية من عصر الصناعة إلى عصر أو مجتمع المعلومات[1]، فالمعلومات رمز من رموز الحضارة الإنسانية ففقدانها يعني فقد الإنسان لذاكرته ومن ثم انتهاء حضارته، فالمعلومات هي أغلى ما يمتلكه الإنسان على مرِّ العصور، ويُعتبر عصر الانترنت أبرز

---

(1) Piragaff (D. K.): Computer crimes and others crimes aganiste information technology in the Canada, report, Rev. int. dr. pen. 1993, p 201.

مظاهر هذا المجتمع المعلومات، بل هو أغلى الثمار، فأهمية الانترنت تأتي من أنه مصدر المعلومات بيد أن الأقاويل والمقالات كثرت في الآونة الأخيرة حول شبكة المعلومات الدولية المعروفة باسم الانترنت، وتم التركيز على الاستخدامات السلبية غير المقبولة دائماً أو غير المشروعة أحياناً حتى أن كلمة انترنت أصبحت عند بعض الناس مرادفة للإباحية والانفلات، وصار الانترنت هو المتهم البريء دائماً في كل مشكلة أو كارثة تحل بالعالم، فبعض مستخدمي الشبكة إما من الجواسيس الذين يحاولون التلصص على الدول أو الهيئات، أو البنوك، أو الأفراد بغية انتهاك حرماتهم أو من الإباحية الذين يريدون عرض بضاعتهم المشبوهة من صور وموضوعات مثيرة على الشبكة، أو من أصحاب العقائد الهدامة، أو الأفكار المنحرفة الذين يحاولون نشرها باستخدام الشبكة أو من قراصنة القرن العشرين الذين وجدوا في الشبكة ضالتهم. وبدأ العلماء والأطباء يُحذِّرون من الآثار النفسية والصحية لمشكلة الانترنت، وظهر الاحتيال عن طريق الانترنت، فقد صاحب انتشار استخدام البطاقات الائتمانية وظهور أنماط إجرامية جديدة لم تكن معروفة استغلتها العصابات الإجرامية المنظمة، فقد رصدت حركة الجريمة الاقتصادية الصور المستحدثة لجرائم البطاقات الائتمانية في مصر، وكان أبرزها الاحتيال عن طريق الانترنت باستخدام بيانات بطاقات ائتمان خاصة بآخرين للتسوق وإجراء بعض المعاملات، وأيضاً جرائم الاحتيال التي تُرتَكب بمعرفة مكتب الاتصالات غير الدولية وغير المرخصة والتي تقوم بتقديم خدمة للمواطن وتحصل منه على مقابل ما، بينما يتم تحميل تكاليف أعباء تلك الخدمة على بعض أصحاب بطاقات الائتمان ثم الحصول على بياناتها بطريق المغافلة فكان الحديث قديماً عن الكوارث الطبيعية كالبراكين والزلازل والأعاصير.... الخ[1] ونعرف ما تُسببه هذه الكوارث من دمار رهيب للبشرية، أما الآن فالحديث له وجهٌ آخر، إذ أصبح الحديث عن الكوارث المعلوماتية نتيجة

(1) ياسين، صباغ محمد محمد، الجهود الدولية والتشريعية لمكافحة الإرهاب وقرب العالم الجديد، دار الرضوان، القاهرة، 2005م.

انحراف تقنيات المعلومات والاتصالات عن مسارها الطبيعي مما مهّد لظهور ما يُسمَّى بالتلوث المعلوماتي، مثل ترويج أفكار الجماعات المتطرفة، المشاهد الجنسية الإباحية، تسهيل العمليات الإرهابية، وعقد صفقات بيع المخدرات، وتسهيل أعمال الدعارة، فهذه الأشياء تُمثّل أعاصير مدمِّرة[1]

نعرض لكم من خلال هذا العمل المتواضع لمفهوم المحكمة الرقمية والجريمة المعلوماتية في الفصل الأول لمفهوم المحكمة الرقمية والجريمة المعلوماتية صور لتكييف القضاء الرقمي وتصنيف الجرائم المعلوماتية وخصائص الجرائم الإليكترونية، وطوائف المجرمون الرقميون. والتنظيم التشريعي للوثائق الإليكترونية. وفي الفصل الثاني نعرض لاختصاصات المحكمة الرقمية، والجريمة المعلوماتية، والاختصاص القضائي في النظام السعودي، كمثال وتنازع الاختصاص واختصاص الجرائم المعلوماتية في النظام السعودي، والاختصاص بنظر الجريمة المعلوماتية، والجرائم المعلوماتية من منظور شرعي وقانوني، والجريمة المعلوماتية في النظام السعودي، وفي الفصل الثالث نعرض لبعض صور للجرائم المعلوماتية، ومنها جرائم الاعتداء على الحياة الخاصة للأفراد عبر الانترنت، وجرائم الاعتداء على الأموال عبر الانترنت، وجرائم القرصنة والتجسس الإليكتروني والإرهاب الإليكتروني، وجريمة انتحال الشخصية عبر الانترنت، وسرقة الملكية الفكرية، وأخيراً المسئولية الجنائية للجرائم المعلوماتية. وفي الفصل الرابع نعرض لإجراءات نظر الجرائم المعلوماتية أمام المحاكم الرقمية، وتحريك الدعوى الجنائية في القانون المصري بوجهٍ عام. ونطاق تحريك الدعوى في جرائم الجلسات وانقضاء الدعوى في القانون المصري، وتحريك الدعاوى في النظام الجزائي السعودي، ومرحلة المحاكمة في نظام الإجراءات الجزائية السعودي، وإجراءات التحقيق وأمر التوقيف، وإحالة الدعوى الجزائية إلى المحكمة المختصة والمحكمة الرقمية، ومشكلة الاختصاص واتجاهات الفقه في

(1) Interpol, Computers and Crime, Manual of Standards and Procedures, 1996.

اختصاص المحكمة الرقمية والمحكمة الرقمية، والحلول المقترَحة بشأن تنازُع الاختصاص، وأخيراً الاتجاهات الإقليمية والدولية ومشكلة الاختصاص. وفي الفصل الخامس نعرض للتحقيق الجنائي والتفتيش في الجرائم المعلوماتية. وفي الفصل السادس نعرض للخبرة والمعاينة في الجرائم المعلوماتية. وفي الفصل السابع والأخير نعرض الإثبات أمام المحكمة الرقمية، والدليل الجنائي الرقمي، وصور الدليل الإلكتروني، وحجية الأدلة الجنائية في الإثبات، والإثبات الرقمي في المسائل المدنية والتجارية والمصرفية، والاتجاه التشريعي بشأن أدلة الإثبات الحديثة وحجيتها، والمشكلات العملية في الإثبات المصرفي بالوسائل المعلوماتية، وأخيراً وسائل فض منازعات التجارة الإلكترونية. ونختم بتطبيقات قضائية على بعض الجرائم المعلوماتية. ثم ملاحق قانون التوقيع الإلكتروني المصري رقم 15 الصادر عام 2004 م ونظام مكافحة جرائم المعلوماتية السعودي.

أسأل الله أن ينال هذا العمل إعجابكم وأن ينفع به أهل العلم في شتى فروع القانون.

عبد الصبور عبد القوي .....



الفصل الأوَّل

مفهوم المحكمة الرقمية

والجريمة المعلوماتية

مقدمة:

المحكمة الرقمية هي نظام جديد من المحاكم المتخصصة تختص بالجرائم الرقمية (المعلوماتية)، وهي على غرار المحاكم المتخصصة كمحكمة الأسرة، ومحكمة الجنايات، والمحاكم المدنية. تتعامل هذه المحكمة مع جرائم الحاسب الآلي ثم تمتدُّ إلى جرائم الشبكات، ومنها شبكة المعلومات الدولية، كما تشمل جرائم الهواتف المحمولة وأجهزة الصرف الآلي. جاءت فكرة إنشاء هذه المحكمة لتلافي القصور في إجراءات التحقيق وعجز الخبرات الفنية لإبداء الرأي في الجرائم الرقمية بما يكتب شهادة الوفاة أو كلمة النهاية للانتظار الطويل والروتين في ساحات المحاكم[1]. أما فهي تختلف عن المحكمة الإليكترونية التي تختص بسير إجراءات التقاضي إليكترونياً، ومن المعروف أن استخراج نسخ إليكترونية من الأحكام مازال يفتقد الاعتراف القانوني لعدم وجود ختم الدولة الرسمي على تلك النسخ، ومن خلال الموقع الإليكتروني يستطيع المتقاضي أن يحصل على معلومات عن سير القضية

(1) هلال، محمد رضوان، المحكمة الرقمية، دار العلوم للنشر والتوزيع، القاهرة 2007م.

ورقم القضية والحكم النهائي دون الحاجة إلى الذهاب إلى المحكمة ودفع مصاريف وإكراميات لسكرتير المحكمة والدخول في دائرة الروتين المعروفة. وداخل قاعة المحكمة الإلكترونية يقوم سكرتير الجلسة بكتابة وقائع الجلسة من أقوال المتهمين والشهود والدفاع باستخدام الكمبيوتر، وهذا بالطبع سيعود بالنفع على الدفاع؛ لأنه يُفضل الحصول على نص وقائع الجلسة بعد انتهاء الجلسة مباشرة وكان النظام السابق لا يوفِّر هذه السرعة. وحول إمكانية استخراج نسخة من حكم المحكمة إليكترونياً، وأنه يجوز استخراج نسخة من الحكم إليكترونياً الآن كما يحدث في مصر، ولكن لن يكون لها قيمة أو مصداقية ولن تعترف بها أي جهة بسبب عدم احتواء عريضة الحكم الإلكتروني على الختم الرسمي للدولة الذي لا يمكن ختمه إلكترونياً إلا إذا تم الاتفاق بين وزارة العدل وهيئة تنمية صناعة المعلومات، أما المحكمة الرقمية فقد تم تطبيقها في كثير من الدول كتجربة ونأمل تعميمها في المستقبل القريب، خاصة وأن الكثير من الدول تأخَّرت بالفعل في تطبيق هذه المحكمة، فقد سبقت دولتان عربيتان قطر والإمارات، فهناك يتم تجديد إجراءات الحبس باستخدام تكنولوجيا في حالة ما إذا كان المتهم مجرماً خطيراً يخشى من حضوره قاعة المحكمة في جرائم المعلوماتية[1]. ولابد الإسراع في نشر هذه التجربة في كثير من الدول كي تعم الفائدة على المواطنين، كما يوصي بأهمية أن تلتزم الدولة بمساعدة المؤسسات المدنية، ورجال الضبط، وخبراء وزارة العدل على التعريف بأهمية قانون الانترنت بجانب قانون العقوبات، وقانون الإجراءات. كما لابد أن نهتم بزيادة عدد المواد الدراسية المتعلّقة بالكمبيوتر والانترنت خاصة بكلية الحقوق والشرطة حتى نوجد جيلاً قادراً على التعامل مع جرائم المعلومات. ويُضاف مؤخراً في بعض الدول العربية إضافة مادة لطلاب الحقوق وهي المرافعة عبر الانترنت، وذلك بالتعاون مع

(1) عوض، رمزي رياض، مشروعية الدليل الجنائي في مرحلة المحاكمة وما قبلها، دراسة تحليلية تأصيلية مقارنة، دار النهضة العربية، القاهرة، 1997م

كلية الحاسبات والمعلومات ويُتيح الجزء العملي بالمادة إمكانية[1]أن فكرة المحكمة الرقمية نشأت على خلفية قصور التحقيق وقصور التكييف القانوني للجرائم الرقمية والتي تزداد يوماً بعد يوم، وتتنوّع الوسيلة التي تستخدم فيها. وزيد على هذا القصور في الخبرة الفنية لإبداء الرأي إذ أن هذه الجرائم مختلفة تماماً عما اعتاد عليها المحققون والقضاة والخبراء[2]. وهذه المحكمة تختص بالجرائم الرقمية DIGITAL CRIMES والتي الأصل فيها هو جهاز الكمبيوتر ثم شبكة الانترنت الدولية والشبكات الأخرى. ويلحق بالجرائم الرقمية الاتصالات التي يدخل معظمها نطاق الكمبيوتر كما يشمل الاختصاص نواتج الأجهزة الرقمية.. وفي إحدى جرائم صرف الأموال من الصارف الآلي ATM بواسطة بطاقة الائتمان ادعى المدّعي أنه بتاريخ معين لم يقم بصرف المبلغ المخصوم من رصيده.. وتصادف وجود كاميرا رقمية مثبّتة قرب الصراف الآلي، وبمراجعة الشريط أمكن ضبط اليوم واللحظة التي تم فيها الصرف. وتم استخراج صور الواقعة بواسطة طابعة كمبيوترية نافثة للحبر لكنها كانت غير واضحة، مما تعذّر معه إبداء الرأي في القضية. وكان على النيابة أن تُرسل الشريط الأصلي المسجّل بواسطة الكاميرا أو نسخة حية منه بدلاً من الصور الكمبيوترية، أو يقوم الخبير بطلبها لإمكان عرضها على الجهاز الخاص بمثل هذه الصور حتى يمكن التحقّق من أن الشخص المدّعي هو الذي قام بالصرف أم غيره ويظهر من استعراض الواقعة السابقة[3].

---

(1) الألفي، محمد محمد، (2007 م)، مؤتمر الحكومة الإلكترونية السادس «الإدارة العامة الجديدة والحكومة الإلكترونية» دبي - دولة الإمارات العربية المتحدة 9 - 12ديسمبر 2007 ورقه عن المحكمة الإلكترونية بين الواقع والمأمول.

(2) علي، عبد الصبور عبد القوي، التجارة الإلكترونية والقانون، دار العلوم للنشر والتوزيع، القاهرة 2007م.

(3) من جريدة مصرس الإلكترونية عبر الرابط.
http://www.masress.com/alalamalyoum/1901106

المبحث الأوّل

مفهوم المحكمة الرقمية

المحكمة الرقمية هي المحكمة التي تختص بالدعاوى الرقمية، وجرائم الشبكات، وتكنولوجيا المعلومات وقضايا الملكية الفكرية والتجارة الإلكترونية وذلك على غرار محاكم متخصصة معينة، كمحكمة الأسرة، ومحكمة الجنايات والمحاكم المدنية. إذاً نستطيع القول بأن المحكمة الرقمية هي المحكمة المختصة بالفصل في الدعاوى الرقمية سواء كانت جنائية، أو مدنية، أو تجارية. لذلك نود أن نقول هل للمحكمة الرقمية علاقة بالمعلومات والاتصالات؟

إن كانت المعلومات هي من صميم عمل المحكمة، وكذلك الاتصالات الرقمية (سلكية ولا سلكية). فهي تشمل التعامل مع أجهزة معينة التي لها علاقة بالقضايا التالية على سبيل المثال:

1 - تتعامل المحكمة الرقمية مع جرائم الحاسب الآلي بصفة أساسية.

2 - الشبكات الدولية.

3 - الهواتف المحمولة.

4 - أجهزة الصرف الآلي.

5 - أجهزة قراءة البيانات.

وإن كنا نود الحديث عن القاضي في تلك المحاكم فهو القاضي البشري، لكنه هو القاضي الذي يُطبِّق القوانين الخاصة بالتعاملات الرقمية، والحكومة الإلكترونية، والتجارة الإلكترونية، والتوقيع الإلكتروني الرقمي، والمستندات الرقمية، وجرائم النصب والسرقة والقتل بالوسائل الرقمية، والعملات

المزيفة الرقمية، والكاميرات الرقمية، وتركيب الصور الرقمية، والشبكات ويعرف مفرداتها وثقافتها[1].

وأما عن الدفاع وتمثيل الخصومة، فالدفاع هو الذي يستوعب التكنولوجيا الرقمية والقوانين الرقمية، ومفردات الجريمة الرقمية، وكيفية سير العمليات الرقمية، والتتابع المنطقي للعمليات المستخدمة في عمليات معالجة البيانات للحصول على نتائج. وهو مَن يعرف عن قرصنة الانترنت، وإطلاق الديدان وكيفية معالجتها، والفيروسات واختراقاتها للأجهزة، والبرامج وكيفية التخلص منها، وأين تختفي الملفات وكيفية إظهارها عن طريق الاسترجاع، وكيفية حماية البرامج وغيرها؟

أما عن شأن المتهم أو المدَّعى عليه في تلك القضايا، فالمتهم هو المجرم المعلوماتي، وهو الذي يُسيء استعمال أجهزة الحاسب والشبكة الدولية والشبكات الأخرى، بإحدى الطرق التي تُعد جريمة يُعاقب عليها القانون. والمجرم المعلوماتي هو مجرم من نوع خاص، إذ أن القراصنة من أذكى أنواع البشر في كل الدول، وهم من المبتكرين والمتجددين، والمجددين للوسائل والطرق، ومن المجرمين الرقميين: الهاكرز.. وغيرهم. خلافاً للمجرم العادي وكما ذكرت أننا الآن انتقلنا من الإجرام العادي إلى الإجرام الرقمي من مجرم إلكتروني خارق الذكاء إلى شخص عادي دفعته العوامل الفسيولوجية، أو الوراثية أو الاجتماعية، أو الاقتصادية لارتكاب الجريمة[2].

---

(1) هلال (2007 م)، محمد رضوان، المحكمة الرقمية، المرجع السابق.

(2) الألفي، محمد محمد، (2007 م)، مؤتمر الحكومة الإلكترونية السادس «الإدارة العامة الجديدة والحكومة الإلكترونية» دبي - دولة الإمارات العربية المتحدة 9 - 12 ديسمبر 2007 ورقه عن المحكمة الإلكترونية بين الواقع والمأمول.

المبحث الثاني

المحكمة الرلكترونية والمحكمة الرقمية والحكومة الإليكترونية

إن مصطلح المحكمة الإلكترونية يُعد من المصطلحات والمفاهيم الحديثة؛ حيث أنه لم يظهر إلا قبيل سنوات بعد انتشار مصطلح الحكومة الإليكترونية، وإذا كان مصطلح الحكومة الإليكترونية يعني بالخدمات الحكومية كافة، فإن مصطلح المحكمة الإلكترونية يختص بخدمات المحاكم فقط[1].

إن مصطلح المحكمة الإليكترونية يعني تفعيل تقنية المعلومات بالشكل الأمثل، بما يُساعد على جودة الخدمات وسرعة إنجازها، كما تنقسم خدمات المحكمة الإلكترونية إلى[2]:

1 – خدمات المواطنين والأفراد g2c.

2 – وخدمات القطاع التجاري g2b.

3 – وخدمات الجهات الحكومية الأخرى g2g.

4 – وخدمات منسوبي وموظفي المحكمة g2e.

إن تطبيق التقنية في الإدارة القضائية بالشكل الصحيح والمتدرج له أثر إيجابي. ويشمل هذا الأثر سرعة الإنجاز للمعاملات والقضايا وتوحيد وتبسيط إجراءات العمل، والمساهمة في أمن المعلومات بحفظها وإتاحة الاطلاع عليها للمصرَّح لهم إضافة إلى ضمان جودة العمل ومواكبة التطور[3].

---

(1) حجازي، عبد الفتاح بيومي، (2002)، الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت، دار الكتب القانونية، القاهرة.

(2) الألفي، محمد محمد، (2007 م)، مؤتمر الحكومة الإليكترونية السادس «الإدارة العامة الجديدة والحكومة الإليكترونية»، المرجع السابق.

(3) راجع الرابط:

www. deirallacity. gov. jo/Seminars_and_workshops/egov/egov_3. doc

إن نجاح التقنية مرتبط بالاهتمام بالعناصر الأخرى المؤثرة في تقديم الخدمات، وهي:

1 - تطوير التقنية.

2 - الموارد البشرية.

3 - وإجراءات العمل.

فبينما تقوم بعض الجهات بمحاولة تحسين مستوى خدماتها من خلال التركيز على العنصر المؤثر الأول بتطوير التقنية، فإننا نجد أنها تغفل عن عنصر فعّال وهام، وهو عنصر الموارد البشرية وذلك بالرغم من أن أساس تحسين مستوى الخدمات، وتُمثّل إجراءات العمل العنصر الثالث الذي لم يراع تحسينه فإن تطبيق التقنية قد يُصبح زيادة في العبء على العمل اليدوي. فيجب التركيز على هذه العناصر الثلاثة، وذلك من خلال الاهتمام بالموارد البشرية، ورفع مستوى منسوبيها فنياً وإدارياً، وعقد الندوات وورش العمل المتخصصة للقضاة وكتاب العدل[1].

إن أنظمة المحكمة الإليكترونية تشمل كلاً من نظام إدارة البوابة الإلكترونية، ونظام المرافعات، ونظام الاتصالات الإدارية، ونظام إدارة القضايا، ونظام التسجيل الصوتي، ونظام إدارة المحتويات، ونظام إدارة الأداء، إضافة إلى إدارة خدمات تقنية المعلومات التحتية من أجهزة وبرامج وأمن المعلومات، وتطبيق المحكمة الإلكترونية يتطلّب العديد من المتطلبات النظامية والإدارية والفنية، بالإضافة إلى الكادر البشري، مثل أنظمة التحقق من الهوية الإليكترونية، وحجية المستندات الإليكترونية، ودعم الإدارة العليا، وإعادة هندسة إجراءات العمل الإدارية، والاهتمام بإدارة التغيير وبنى الاتصالات التحتية، وتطوير الموظفين وغير ذلك[2].

(1) علي، عبد الصبور عبد القوي، التنظيم القانوني التجارة الإلكترونية، المرجع السابق.

(2) سلامة، محمد عبد الله أبو بكر (2006. م)، جرائم الكومبيوتر والانترنت موسوعة جرائم المعلوماتية، منشأة المعارف، الإسكندرية.

ولا ننكر ومواكبة وزارات العدل في بلادنا العربية لمقتضيات الحكومة الإليكترونية من خلال استخدام الحاسب الآلي في المحاكم اتجاه محمود، ولافت للانتباه أكثر مما لو قامت بذلك وزارة المالية أو التخطيط على سبيل المثال، ذلك لأن الحاسب الآلي جزء مهم منهما بالأصالة، ومن طبيعة وواقع عمل هذه الوزارات، إما أن تستحدث وزارة العدل نظاماً إليكترونياً يتوافق مع طبيعتها ومهامها بشكر القائمون عليه. واتجاه الوزارات جميعاً لتطبيق نظام الحكومة الإليكترونية أمر مطلوب، وأصبح ضرورياً في عصر أخذ يعتمد على الحاسب الآلي في كثير من معاملاته إن لم يكن فيها كلها، وقد سعت الكثير من الجهات الحكومية في بلادنا منذ فترة ليست قصيرة لتوسيع نطاق الحكومة الإليكترونية، ليشمل جميع أجهزة الدولة، لما لذلك من فوائد مهمة للمواطن، الذي قد يقوم بكل إجراءاته ومعاملاته من البيت أو العمل وبكل دقة وإتقان وسرية، بعيداً عن أي محسوبيات أو وساطات. والحكومة الإليكترونية رغم أنها غير آدمية إلا أنها أخلاقية إلى حد كبير، حيث تتوافر فيها مجموعة قيم قد نفتقدها في بعض الكوادر البشرية بين الحين والآخر، فهي عملية جميلة جداً، ومحايدة جداً، ولا تتعاطف مع هذا أو ذاك، أو تجامل هذا على حساب ذاك، كما تتوافر فيها الشفافية بحيث لا تُقدِّم مصلحة مواطن على حساب آخر، أو تتلقى رشوة لتمرير مصلحة مواطن وتعطيل مصلحة آخر، أو تنتهك قوانين الدولة وتؤثِّر على الصالح العام، وبهذا فهي نزيهة وصادقة وأمينة ومخلصة ومتجرِّدة من الأغراض وأطماع الدنيا الزائلة. وحيث أن خدمات وزارات العدل ونظامها الإليكتروني، ينجز المعاملة في دقائق معدودة بواسطة الحاسب الآلي[1].

فهناك مصالح تظل معطلة لفترات طويلة لأن الإجراءات البيروقراطية والكم الهائل من القضايا يجعل النظر إليها ثقيلاً، في الوقت الذي نعيش عصراً سريعاً يحتاج حسماً سريعاً للنزاعات، وفي جميع الأحوال تبرز الحاجة

(1) الأمين، محمد (1997م)، العدالة الجنائية ومنع الجريمة، دراسة مقارنة، ط1، أكاديمية نايف العربية للعلوم الأمنية – الرياض.

إلى هذا النظام الجديد في المعاملات وإحالة القضايا آلياً بين القضاة، ويلازم ذلك تحديث الأنظمة القضائية القديمة، كي تتماشى مع التنظيم القضائي الجديد في الدول العربية وكي تتماشي مع الحكومة الإلكترونية، وهذا التطوُّر والتطوير مطلوبان ولهما جدواهما المستقبلية والحياتية ولابد من مواكبة العصر ومتغيرات الزمن، فمن حق بلادنا وهي تعيش هذه النهضة أن تكون مواكبة لروح العصر شكلاً ومضموناً، فالحكومة الإلكترونية منهج دولة وتطلعات قيادة وطن ومواطن، ولابد أن ترقى جميع أجهزة ومؤسسات الدولة إليها، فهي باختصار نظام عملي وعلمي ومنهجي، يوفر فرصة للعمل بأفق إداري أكثر احترافية، ويقوم على الإدارة العلمية وتغليب مفاهيم النظام والموضوعية، ويرتقي بالروح العملية للموظفين، ويُكسبهم مهارات أكثر في تنظيم المعلومات والدقة والإنجاز، وكذلك في تطوير القدرات؛ ذلك لأن الحكومة الإلكترونية تطور قدرات الموظفين، وتُفجِّر طاقاتهم الإبداعية، وتُخضِعهم للمحاسبة الفورية في حالة تعطيل الأعمال، أو التراخي في القيام بالمهام، أي تجعل الكادر البشري أكثر التزاماً ومسئولية وعطاء، إن لم يكن لأجل الوظيفة والعمل والوطن، فمن أجل تطوير النفس ولعل ابرز تطبيق لذلك تعميم البصمة الإلكترونية في كثير من المؤسسات والمصالح الحكومية[1].

أما المحكمة الرقمية فهي محاكم متخصصة في النظر في القضايا التي تُرتكب عبر الوسائط الإلكترونية سواء كان أطراف الخصومة شخصاً طبيعياً أو اعتبارياً كالسطو على حقوق الملكية الفكرية لأحد شركات البرمجيات أو سلب حقوق الملكية الفكرية.

(1) الشاذلي، فتوح وعفيفي، كامل عفيفي، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون (دراسة مقارنة) منشورات الحلبي الحقوقية، بيروت – لبنان،

المبحث الثالث

التحول إلى نظم القضاء والعدالة الإلكترونية كبداية لنشأة المحكمة الرقمية

خلال السنوات الأخيرة سعت المحاكم في كثير من الدول العربية في مجال التطبيقات الإلكترونية عبر استخدام كافة الوسائط والتقنيات المتوفرة لخدمة مرفق العدالة الذي راهن كثيرون في وقت سابق على صعوبة دخول هذه التقنيات لمجال العدالة الذي يتطلب قيوداً وإجراءات معينة تُنظّمها القوانين والأنظمة[1].

ولأن حجم التقنيات التي ستطوع لخدمة مرفق العدالة كبيراً لدرجة أن المحاكم بدأت إلى حد كبير تنافس دوائر تعتبر التقنيات الحديثة جزءً لا يتجزأ من عملها. فالمطلوب استخدام التقنيات بتنوع الخدمات الإلكترونية التي حظيت بإطار فعّال وسلس لمتابعة وتطوير عملية التحويل الإلكتروني لتحتل مكانها الذي حدّدته من خلال خططها الاستراتيجية ضمن مبادرة الحكومة الإلكترونية، ويهدُف هذا النظام إلى تحسين أداء العاملين وتوفير منظومة عمل وإدارة عبر شبكة معلوماتية للموارد البشرية والمالية وفق تكنولوجيا إدارية بما يُحقق الاستثمار الأمثل للموارد[2].

متطلبات التحول إلى نظم المحكمة الإلكترونية:

1 - استخدام تكنولوجيا المعلومات بأكبر نسبة من مجمل إجراءات العمل في المحاكم في أجهزتها القضائية والإدارية والمالية.

2 - أهمية مواكبة مستجدات تكنولوجيا العصر، لتكون نموذجاً يُحتذى

---

(1) هلال، محمد رضوان، المحكمة الرقمية، المرجع السابق.

(2) الألفي، محمد محمد، (2007 م)، مؤتمر الحكومة الإلكترونية السادس «الإدارة العامة الجديدة والحكومة الإلكترونية» دبي – دولة الإمارات العربية المتحدة 9 – 12 ديسمبر 2007 ورقه عن المحكمة الإلكترونية بين الواقع والمأمول.

به في الخدمات القضائية والقانونية والبحثية الإلكترونية.

3 - تحسين تقديم الخدمات والتقنيات عن طريق استحداث خدمات جديدة والارتقاء بالبرامج والأنظمة المقدمة لكافة فئات المتعاملين معها[1].

4 - تحديث موقع المحاكم على الانترنت وتطويره:

أ - إطلاق بعض محتوياته باللغة الإنجليزية.

ب - التطوير في الموقع ويشمل الأدلة التي تُوضح أصناف الدعاوى.

ج - التوكيلات القانونية.

د - توثيق العقود.

هـ - توضيح درجات التقاضي والتقسيمات النوعية والقيمة للقضايا.

و - تبين الخدمات الإلكترونية كافة ومتطلباتها وخطواتها.

ل - وجود بيانات تحتويها قوائم بأسماء وعناوين المحامين والمأذونين الشرعيين.

ز - لا بد أن يحتوي الموقع على نصوص التشريعات المختلفة من دستور ومراسيم وقوانين ونظم ولوائح وتعاميم وأوامر وغيرها.

ذ - ويشمل كذلك محتويات متغيرة كالإعلانات والأخبار ذات الصلة بالمحاكم وموقع المحاكم.

ك - معلومات حول إدارة المعرفة القضائية والقانونية.

---

(1) الأمين، محمد (1997م)، العدالة الجنائية ومنع الجريمة، دراسة مقارنة، ط1، أكاديمية نايف العربية للعلوم الأمنية - الرياض.

5 - العمل على التوعية بثقافة وفكر الشفافية والجودة والعمل بنظام الاقتراحات والشكاوى الإلكتروني.

6 - الاهتمام بتنمية الموارد البشرية وإكسابها المهارات المختلفة في إطار الاستغلال الأمثل للأتمتة وتقنية المعلومات.

7 - تقديم خدمة البث الإلكتروني العاجل من قبل المحاكم الإلكترونية لكل جديد من أخبار المحاكم وتشريعاتها وقراراتها.

8 - توفير قناة تواصل يتواصلون من خلالها مع المحاكم عبر خدمة الاستعلامات الإدارية (info) وبواسطتها يستعلمون ويستفسرون ويتساءلون عن إجراءات أو بيانات أو معلومات هم بحاجة إليها من خلال هذه الخدمة وبعضهم يتقدمون بطلبات وظائف وأمور أخرى[1].

ولا شك في أن تطور مفهوم التقاضي الإلكتروني كان ولازال له الدور الهام بالنسبة للقضاة والمحامين وسبب رئيس في استقلال المحكمة الرقمية عن المحاكم العامة، ويظهر ذلك في عدة أمور:

1 - توفير مجموعة من الخدمات الإلكترونية للقضاة، وأهمها قاعدة إدارة المعرفة القضائية القوانين والمبادئ القانونية والأحكام والتي تُعتبر أداة قيمة للقضاة لتسهيل عملهم وسرعة الوصول إلى المعرفة المطلوبة لاتخاذ القرارات والأحكام المناسبة.

2 - توفير مجموعة من الخدمات لإدارة قضاياهم وجلساتهم وأحكامهم وأدوات لقياس أدائهم.

3 - أن تقدّم المحاكم للمحامين عدداً من الخدمات الإلكترونية

(1) سلامة، محمد عبد الله أبو بكر، (2006. م)، جرائم الكومبيوتر والانترنت موسوعة جرائم المعلوماتية، منشأة المعارف، الإسكندرية.

تُساعدهم في متابعة القضايا الخاصة بمكاتبهم حيث بالإمكان الاطلاع على جدول جلسات قضاياهم بالإضافة إلى متابعة طلباتهم والتنفيذيات التي تمت عليها، مما يُسهل عليهم إجراءاتهم، ويوفر الوقت والجهد في عملهم، عوضاً عن مراجعة المحاكم دون مغادرة مكتبه.

4 - تقديم خدمات إلكترونية عديدة عن معلومات جميع القضايا التي كلّف بها الخبراء لأداء رأي الخبرة بحيث توفر لهم هذه الخدمات سهولة في متابعة أعمالهم والاستفسار عنها ومعرفة متطلباتها.

5 - توفير خدمة إمكانية أطراف الدعاوى الاطلاع على معلومات قضاياهم خلال مراحل التقاضي[1].

ولا شك في أن المتابع لحركة التطوُّر التقني التي تعيشها الدول العربية بكافة دوائرها الحكومية والخاصة، يلمس أن العديد منها باتت تتسابق لتطوير هيكلها سواء الإداري أو التقني لمواكبة آخر التطورات لتُقدم أفضل ما لديها خدمة للعاملين فيها والمتعاملين معها. ويعرف أن هاجس الحكومة الإلكترونية التي أطلقت في الدول العربية قبل سنوات بات يُشكل جهاز الرقيب على كل دائرة، إذ ذهبت الدوائر على اختلاف أوجه عملها تسعى لاستحداث كل ما يمكن لتطوير نفسها وتقديم أفضل ما لديها، إذ أن تخلفها عن اللحاق بركب باقي الدوائر سيجعلها في مرحلة متأخرة، قد تؤدي إلى شل حركتها في كيفية التعامل مع باقي زميلاتها فضلاً عن إحداث فجوة سيدفع ثمنها الجميع. والمراقب لعمل الدوائر الحكومية يلحظ أنها أصبحت قاب قوسين أو أدنى من تطبيق معايير الحكومة الإلكترونية بشكل متكامل، إذ عمدت جميع الدوائر وبدرجات متفاوتة إلى تطوير أنظمتها التقنية وتحديث مواقعها

(1) علي، عبد الصبور عبد القوي، التنظيم القانوني التجارة الإلكترونية، المرجع السابق.

الإلكترونية، لتصبح قادرة على التعامل مع هذا الرقيب الجديد[1]، الذي يلمس أي تقصير فيه المتابع والمراجع قبل المسئول نفسه. ويرى العديد من المسئولين أن رقابة الرأي العام أصعب أنواع الرقابة، ويحمل المقصِّر أعباء ثقيلة التي باتت تُشكِّل هاجساً لجميع مديري الدوائر خاصة وأنها تحظى بمراقبة ومتابعة حثيثة من القيادات وأصبحت وزارات العدل في الدول العربية واحدة من وزارات الحكومة سعياً نحو التقنية، إذ سخَّرت كل المتاح لخدمة مرفق العدالة فيها، الذي راهن الكثيرون على صعوبة استخدام التقنيات في هذا المرفق لخصوصيته واحتكامه لقوانين وتشريعات يُعتبر الخروج عليها مخالفة للقانون، وقد تؤتي نتائج عكسية[2].

(1) الكركي، كمال، جرائم الحاسوب ودور مديرية الأمن في مكافحتها، ورقة عمل مقدمة إلى ندوة قانون حماية حق المؤلف، نظرة إلى المستقبل، المنعقدة في عمان بتاريخ 1999/7/5م.

(2) حجازي، عبد الفتاح بيومي، (2002)، الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت، دار الكتب القانونية، القاهرة .

المبحث الرابع

نظم المحاكمة الرقمية وتطبيقه على الجرائم المعلوماتية

في هذا الاتجاه تم دراسة فكرة إمكانية عقد محاكمة عبر الوسائل التقنية في أي وقت وأي مكان وتتمثّل الفكرة الجديدة في:

1 - أن يُناوب قاضٍ وبشكل يومي سواء في بيته أو في مكتبه، لنظر القضايا البسيطة التي تحدث كل ليلة، وهي كالمخالفات والحوادث المرورية، وتناول المشروبات الكحولية، وما إلى ذلك من جرائم يحكم في أغلبها بالغرامة.

2 - بعد ضبط المتهم من قِبل دورية الشرطة ونقله إلى المركز يتم في أغلب الأحيان حجزه في الزنزانة إلى اليوم التالي لعرضه على وكيل النيابة، وقد يضطر للمبيت عدة أيام إذا كانت مخالفته أو الجرم الذي ارتكبه وقع في نهاية الأسبوع، وهو ما يعتبر وقتاً وعملاً على رجال الشرطة ومن بعدهم النيابة العامة ثم المحاكم، وتأخذ قضيته وقتاً طويلاً وتستنفد جهوداً كبيرة، ويحكم على المتهم في آخر المطاف بالغرامة[1].

3 - في إطار فكرة «القضاء الإليكتروني» بعد ضبط المتهم يتم الاتصال بالقاضي وهو في بيته عبر كاميرا، شريطة أن يُزود كل مركز شرطة بكاميرا أيضاً لمشاهدة المتهم من قِبل القاضي، وتكون هذه العملية بحضور أحد وكلاء النيابة العامة الذين يناوبون بشكل يومي في مراكز الشرطة، وبعد اطلاع القاضي على حيثيات القضية بإرسال أوراقها إليه في منزله أو مكتبه

(1) شتا، محمد محمد، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، 2001م.

بواسطة البريد الإليكتروني، يصدر حكمه على المتهم، وينفذ الحكم فوراً، ويسلم المتهم نسخة منه بعد أن يرسله القاضي إلى مركز الشرطة بواسطة البريد الإليكتروني أيضاً. والولايات المتحدة الأمريكية عمدت إلى تطبيق مثل هذه التجارب، وأن وزارات العدل في الدول العربية لا ينقصها الإمكانيات والتقنيات لاستحداث ذلك، في القضايا الجزائية البسيطة فقط، وأن الأمر يحتاج إلى تشريع خاص لهذه المسألة، وهو ليس بالصعب إذا ما ربط بالتشريعات المتطورة كالتوقيع الإليكتروني وغيره[1].

4 - فإذا ما نظرنا إلى تكلفة الموقوف على ذمة هذه القضايا بأن السجين يُكلف الدولة نحو 40 دولاراً من طعام وشراب وعلاج وغيرهما، فإن هذا الأمر سيوفر على الدولة الكثير، خاصة وأن أي إنسان معرَّض لأن يُصبح من وجهة نظر القانون متهماً، إذ قد يرتكب فعلاً يُعاقب عليه القانون[2].

5 - سيضطر مركز الشرطة إلى حجزه حتى الصباح لعرضه على وكيل النيابة، ثم يُحوَّل بعدها إلى المحكمة لتأخذ القضية دورها حسب الجدول، ويضطر المتهم إلى توكيل محام وتعطيل أعماله، أما في حال تم تطبيق «القضاء الإليكتروني» فإنه سيصار إلى حكمه في نفس الوقت وعودته إلى منزله، ويكون قد نال عقابه على الفعل الذي ارتكبه، وأكد أن تطبيق هذه الفكرة سيوفر على الدولة الكثير، خاصة وأن مراكز حجز المتهمين تزخر بالمحجوزين على ذمم قضايا تصنف من وجهة نظر القضاء بالسيطرة.

---

(1) N.T.I.C (1: "les nouvelles technologies de l'information et de la communication".

(2) الألفي محمد محمد، (2007 م)، مؤتمر الحكومة الإلكترونية السادس «الإدارة العامة الجديدة والحكومة الإلكترونية»، دبي – دولة الإمارات العربية المتحدة 9 – 12 ديسمبر 2007 ورقه عن المحكمة الإلكترونية بين الواقع والمأمول.

6 - حيث أن تطبيق هذه الأمر سيوفر على القضاء أجرة نقل متهمين ومراكز توقيف وحراسة وتكلفة توقيف وإشغال أوقات وكلاء النيابة العامة والقضاء، وستؤدي بالتالي إلى زيادة الضغط على المحاكم.

7 - ومن أوجه التطوُّر التي يجب تفعيلها في نظم المحاكمة الإلكترونية حول إعلان المدَّعى عليهم عبر الفاكس أو البريد الإلكتروني والبريد المسجَّل، وتخدم فكرة «القضاء الإلكتروني» إذا ما تم الأخذ بها، فكرة العدالة الجنائية ضرورة سرعة الفصل في القضايا وإعادة الحقوق إلى أصحابها في أسرع وقت. إلى ذلك تبقى المسألة مجرد فكرة تُطرح على بساط البحث لتبقى عملية الأخذ بها وإقرارها مناط بالمسئولين، إذ أن الأخذ بها يحتاج فعلاً إلى تعديل في قانون الإجراءات الجزائية أو استحداث تشريع خاص لهذه المحاكمة[1].

---

(1) سلامة، محمد عبد الله أبو بكر (2006. م)، جرائم الكومبيوتر والانترنت موسوعة جرائم المعلوماتية، منشاة المعارف، الإسكندرية.

المبحث الخامس

إدارة الدعوى الإلكترونية ودوره في الجرائم المعلوماتية

المطلب الأوّل

أهداف مشروع الدعوى الإلكترونية

إن تطبيق مشروع إدارة الدعوى الإلكترونية في الدول العربية يؤدي إلى تحقيق الأهداف التالية:

1 - دعم القدرات المؤسسية لوزارات العدل وإدارة المحاكم عن طريق تدريب العاملين وتحديث نظم العمل في المحاكم، وذلك بالتحديث بالكامل بإدخال أنظمة إدارة الدعوى الإلكترونية وتدريب العاملين على استعمالها مع إعادة هندسة الإجراءات والدورة المستندية للقضية بغرض تبسيطها والإسراع بعملية الفصل في القضايا[1]، وكذلك أحكام الرقابة عن طريق تمكين التفتيش القضائي من الإطلاع على نسبة الفصل في القضايا بصورة يومية ومكثفة مع التعرف الفوري على أسباب البطء في التقاضي أو التأجيلات.

2 - تطوير نظم الإطلاع على المعلومات القضائية والقانونية سواء فيما يتعلق بالقوانين أو الأحكام الصادرة من المحاكم، خاصة المحكمة العليا عن طريق إدخال أنظمة البحث الإلكتروني وتطوير قاعدة معلومات قضائية إلكترونية متكاملة وشاملة.

3 - تقصير أمد التقاضي والتيسير على المتقاضين، مما يؤدي في النهاية إلى دقة الأحكام وتطابقها مع صميم القانون في الغالب الأعم مع

---

(1) الألفي، محمد محمد، (2007 م)، مؤتمر الحكومة الالكترونية السادس «الإدارة العامة الجديدة والحكومة الإلكترونية» دبي - دولة الإمارات العربية المتحدة 9 - 12 ديسمبر 2007 ورقه عن المحكمة الإلكترونية بين الواقع والمأمول.

تحسين سبل الوصول إلى العدالة للمواطنين والفقراء والنساء[1].

4 - زيادة الوعي القانوني والقضائي لدى العامة والنساء والطبقات الفقيرة عامة والأميين منهم خاصة عن طريقة عمل الحلقات التعليمية والدورات التثقيفية لهم وتوزيع المطبوعات المحررة بلغة سهلة الفهم والتي تناسب كافة طبقات المجتمع.

5 - دعم قدرات النساء والطبقات المعوزة على الاستعانة بالنظام القضائي للدفاع عن حقوقهم عن طريق النظر في إيجاد نظام قضائي مناسب للمساعدة القضائية والتقليل أو الإعفاء من الرسوم القضائية لهذه الفئات المحتاجة[2].

أهمية تطوير نظم التعليم القضائي عن طريق العمل مع المعهد العالي للقضاء بتحديث المناهج الدراسية وتعميمها. وحيث أن الفئات المستفيدة من مشروع إدارة الدعوى الإلكترونية جمهور المتقاضين في وزارة العدل بصفة عامة، والجهات غير الحكومية العاملة في هذا المجال.

المطلب الثاني

صور لتطبيق القضاء الرقمي

كان لنا أن نتعرَّض لبعض الصور لتطبيق القضاء الإلكتروني في الدعاوى الرقمية:

---

(1) عرب، يونس، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، منشورات اتحاد المصارف العربية، الطبعة الأولى، 2000م.

(2) هلال، محمد رضوان، المحكمة الرقمية، المرجع السابق.

1 - «قاضٍ إلكتروني» لسرعة حسم القضايا في البرازيل[1]

التكنولوجيا في مجال القانون والقضاء انتشرت مؤخراً في البرازيل من خلال برنامج حاسوبي يعتمد على الذكاء الاصطناعي أُطلق عليه اسم «القاضي الإلكتروني». ويهدُف هذا البرنامج الذي يوجد على جهاز حاسب محمول إلى مساعدة القضاة المتجوِّلين في تقويم شهادات الشهود والأدلة الجنائية بطريقة علمية في مكان وقوع الجريمة، ثم يقوم بعد ذلك في المكان نفسه بإصدار الحكم بالغرامات إن اقتضت الجريمة ذلك، وقد يوصي بالسجن أيضاً. والبرنامج جزء من خطة أُطلق عليها «العدالة على عجلات»، التي تهدُف إلى تسريع البتّ في القضايا المتراكمة في البرازيل، وذلك بالحكم الفوري في الحالات غير المعقّدة.

فمعظم المواطنين يشعرون بالسعادة عند البت في القضايا في الحال، مشيرًا إلى أن الفكرة لا تعني أن يحلّ البرنامج محلّ القضاة الحقيقين، ولكن ليجعل أداءهم أكثر كفاءة.

إن معظم حالات الحوادث الصغيرة التي يُطلب فيها البتّ بسرعة تتطلّب بعض الأسئلة البسيطة فقط دون الحاجة إلى تفسير القانون، ذلك أن عملية تحديد الحكم تعتمد على المنطق المحض حال وصول فريق العدالة المحمولة إلى موقع الحادث خلال 10 دقائق. فالبرنامج الجديد يقدِّم للقاضي عدة أسئلة بأكثر من خيار للجواب عنها؛ مثل: «هل توقف السائق عند ظهور الضوء الأحمر»، وهل كان السائق قد تعاطى المشروبات الكحولية فوق المعدَّل الذي حدّده القانون؟ » وغيرها من الأسئلة التي لا تحتاج إلا الإجابة بنعم أو لا ثم يصدر الحكم بعد ذلك. ونوّه إلى أن البرنامج يطبع مبررات الحكم إلى جانب الأحكام البسيطة مؤكداً إمكانية تجاوز الحكم الذي يصدره البرنامج

(1) الشاذلي، فتوح وعفيفي، كامل عفيفي، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون (دراسة مقارنة) منشورات الحلبي الحقوقية، بيروت – لبنان،

إن اختلف مع رأي القاضي البشري[1].

2 - «وفي بلجيكا.. نحو قضاء إلكتروني»:

في 2005 م صدرت مبادرة لسنّ تشريع القضاء الإلكتروني في بلجيكا حيث رسخ إطاراً تشريعياً واضحاً يمنح المحاكم والمؤسسات القضائية والعاملين قدرة الاتصال وتبادل الوثائق الرسمية بوسائل إلكترونية؛ وخدمات الدفع الإلكتروني أيضاً، للاختبار في النصف الأول من العام 2005 م.

وتأمل الحكومة الإلكترونية البلجيكية أن يوفر هذا الإنجاز فوائد ملموسة للمواطنين من حيث تكاليف أقل وإجراءات أسرع وأبسط.

3 - «التقاضي الإلكتروني في الصين»:

ففي مدينة زيبو – في إقليم شاندونج – توجد محكمة «إلكترونية» أصدرت خمسة آلاف حكم قضائي بهذه الطريقة. وهي تعتمد على برنامج كمبيوتري متطور يحفظ كافة القوانين والأنظمة، وظروف الإدانة المحتملة، والقضايا المماثلة التي صدر فيها حكم سابقاً.. وقبل الاحتكام للقاضي الإلكتروني يُعد الدفاع والادعاء معطياتهما على قرصين يملكان نفس السعة وقد يطلب القاضي الإلكتروني رأي القاضي البشري بخصوص بعض التفاصيل الخاصة قبل أن يقوم بإصدار الحكم والعقوبات المفروضة !! ومن محاسن الحكم بهذه الطريقة (غير أنها جماعية وتتضمن عقوبات قياسية موحدة) أن الكمبيوتر لا يملك عواطف أو ميولاً أو مواقف مُسبقة، ويعمل بطريقة مجرَّدة بعيدة عن أي تأثير خارجي.
– وفي جميع الأحوال يظل في مقدور قضاة الاستئناف تعديل الأحكام التي يطلقها الكمبيوتر وإدخال رؤيتهم الإنسانية لكل قضية على حده (وهو ما يُساهم في إثراء البرنامج وجعله أكثر خبرة ومرونة !! أما من الناحية التقنية البحتة فأتصور أن برنامجاً كهذا يتضمَّن بالضرورة عدداً كبيراً من العمليات المنطقية

(1) N.T.I.C.I: "les nouvelles technologies de l'information et de la communication".

المترابطة مثل (إذا ضرب زيد عمر/يدخل زيد السجن ويدفع تعويضاً لعمر). ولكن في حال اكتشف الكمبيوتر أن (عمر هو من تحرش أولاً بزيد) سيكتفي حينها بإصدار حكم مخفف (بسجن زيد دون تعويض عمر هذا الترابط المنطقي يمكن برمجته لخدمة أي مجال نظري آخر يمكن تصوره.. إذ يمكن مثلاً برمجة الكمبيوتر ليعمل طبيباً في الأمراض البسيطة والشائعة اعتماداً على ترابط من نوع (في حال التهاب اللوزتين/تناول مضاد أموكسيل لسبعة أيام)، ولكن (في حال كان طفلاً/وتكرر التهاب اللوزتين/يستحسن إزالتهما نهائياً... وفي المستقبل القريب - ظهور أجهزة قادرة على تشخيص وعلاج الأمراض الشائعة دون الحاجة لمقابلة الطبيب؛ إذ سيكون بإمكانها تشخيص المرض وصرف الدواء وإسداء النصائح - وإضافة المعلومات إلى أرشيف المريض - بشكل أسرع وأكثر فعالية من معظم الأطباء.. وبعد عشرين عاماً من الآن لا أستبعد انتشارها في الشوارع (كماكينات بيع المرطبات)؛ بحيث يمكنك إدخال سن المريض وجنسه ومواصفات الحالة فتخرج لك روشتة بالدواء المناسب (أو ربما ستفاجئك بإخراج الدواء نفسه!! وكما يصعب ترك القرار للكمبيوتر وحده في القضايا الجنائية الكبيرة؛ يصعب ترك القرار له في الحالات المرضية المعقدة أو التي تتطلّب خبرة طبية متقدمة (... أقول هذا من باب الحذر والافتراض بأن أجهزة المستقبل ستجمد عند مستوى تقني معين!![1]

4 - «بداية فكرة محكمة لتسوية الخلافات على الانترنت في العالم»:

افتُتحت في سنغافورة عام 2000 م افتتحت أول محكمة من نوعها في العالم على الانترنت متخصصة في تسوية الخلافات المتعلقة بالتجارة والأعمال الإلكترونية على شبكة العنكبوت الدولية (الانترنت)، وكانت بمثابة آلية لفض النزاعات في هذا النوع الجديد من الخلافات التجارية والمالية دون الحاجة إلى

(1) N.T.I.C.1: "les nouvelles technologies de l information et de la communication".

المحكمة التقليدية، وهو أمر فرضته طبيعة التجارة الإلكترونية والتباعد الجغرافي بين التجار والشركات، أو بين الشركات وزبائنها، وستكون هذاهالخدمة سريعة، وهذه ميزة أخرى تتناسب مع السرعة التي تتميز بها التجارة الإلكترونية عن التجارة التقليدية، كما ستكون مجانية، عدا رسوماً رمزية جداً.

لكن التجربة طرحت أهمية اعتراف السلطات الأمنية والتجارية بها وبأحكامها لتتمكن المحاكم الإلكترونية من فرض أحكامها حينذاك بشكل كامل، وللوصول إلى قوانين دولية للتجارة الإلكترونية خلال السنوات القادمة، ومع أن عدداً من الشركات الاستشارية الأمريكية قد بدأت عرض خدماتها لفض النزاعات التي لا تدخل في نطاق المحاكم التقليدية، فإن أحداً لم يقم بتأسيس محكمة بديلة لفض النزاعات على الانترنت مباشرة مثل التي افتتحت في سنغافورة، إن افتتاح هذا النوع من الخدمة القانونية الجديدة يتماشى مع سعي سنغافورة لتكون مركزاً إقليمياً وعالمياً للتجارة الإلكترونية، وستقدم المحكمة الإلكترونية السنغافورية خدماتها على أساس آليات المحاكم الثانوية وبالاشتراك مع سبع جهات قانونية، على رأسها وزارة العدل السنغافورية، والمجلس الاقتصادي والتنموي في الجزيرة، ومحاكم الخلافات الصغيرة، ومركز فض النزاعات السنغافوري، والمركز الدولي السنغافوري للوساطة. هي ليست محكمة للبت في أية قضايا أخرى إجرامية أو اجتماعية أو غير ذلك؛ لصعوبة تحويل مؤسسة القضاء بكل أعمالها إلى الانترنت في الفترة الحالية، ومن ذلك اختصاص المحاكم التقليدية بخلافات التجارة التقليدية[1]

وتُمثّل الجرائم المعلوماتية تحدياً كبيراً لإدارة نظم المعلومات لما تُسببه من خسارة كبيرة وبشكل عام يتم التمييز بين ثلاثة مستويات للجرائم المحوّسبة وهي:

سوء الاستخدام لجهاز الحاسب: وهو الاستخدام المقصود الذي يمكن أن يُسبب خسارة للمنظمة أو تخريب لأجهزتها بشكل منظم.

(1) N.T.I.C.1: "les nouvelles technologies de l'information et de la communication".

المبحث السادس

الجريمة المعلوماتية (الرقمية) وتصنيفها

المطلب الأوّل

مفهوم الجريمة المعلوماتية (الرقمية)

الجريمة المعلوماتية (الرقمية) هي نشاط غير مشروع موجّه لنسخ، أو تغيير، أو حذف، أو الوصول إلى المعلومات المخزّنة داخل الحاسب أو التي تحول عن طريقه، وهي جريمة عابرة للحدود لا تعترف بعنصر المكان والزمان فهي تتميز بالتباعد الجغرافي[1].

الجريمة المعلوماتية (الرقمية): هي عبارة عن سوء استخدام لأجهزة الحاسب بشكل غير مشروع يؤدي إلى ارتكاب جريمة تعاقب عليها الأنظمة والقوانين خاصة بجرائم الشبكات وتكنولوجيا المعلومات، فالجرائم المتعلقة بالحاسب هي الجرائم التي تستخدم فيها الحاسب والوسائط الإلكترونية كأداة لتنفيذ الجريمة[2].

والجريمة المعلوماتية (الرقمية) نمط من أنماط الجرائم المعروفة في قانون العقوبات مرتبط بتقنية المعلومات وقد تتّصف بإدخال بيانات مزورة في الأنظمة. وإساءة استخدام المخرجات، وأثرها سريع الزوال وصعب التعقب، كما قد تكون وسيلة للغش والتحايل والاعتداء، إضافة إلى أن التجهيزات

---

(1) علي عبد الصبور عبد القوي، الجريمة الإلكترونية، دار العلوم للنشر والتوزيع، القاهرة 2007م.

(2) بيومي، حجازي عبد الفتاح، جرائم الكمبيوتر والانترنت، دار الكتب القانونية، القاهرة، 2005م.

والبرمجيات الإليكترونية تكون نفسها محلاً للاعتداء كالدخول غير المشروع والاطلاع أو تعديل أو تخريب البيانات(1).

والجريمة المعلوماتية (الرقمية) هي كل فعل ضار يأتيه الفرد عبر استعماله الوسائط الإليكترونية مثل الحاسبات، أجهزة الموبايل، شبكات الاتصالات الهاتفية، شبكات نقل المعلومات، شبكة الانترنت، كتدمير بيانات وحواسيب الغير بواسطة فيروسات أومحاولة الوصول غير المشروع لبيانات سرية غير مسموح بالاطلاع عليها، ونقلها، ونسخها، أو حذفه.

والفقرة الثامنة من المادة الأولى من نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية تنص على أن المقصود بالجريمة المعلوماتية: «أي فعل يرتكب متضمناً استخدام الحاسب الآلي، أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام».

ولكن يصعب الوصول إلى تعريف جامع للجريمة الإليكترونية وذلك بسبب التطور السريع في وسائل تقنية المعلومات بالإضافة إلى تنوُّع أساليب ارتكابها وظهور أشكال جديدة ومستحدثة وكذلك اختلاف الزاوية التي ينظر من خلالها مَن يحاول أن يعرفها. وقد آثر المعرفين إلى وضع تعريف للجريمة الإليكترونية ككل بشكل عام دون تحديد التفاصيل تحسباً للتطور التقني والعلمي في المستقبل، ويمكن أن تتم تلك الجرائم سواء من قبل أشخاص خارج الدولة ويقومون باختراق نظام الحاسب من خلال الشبكات أو من قبل أشخاص داخل الدولة يملكون صلاحيات الدخول إلى النظام ولكنهم يقومون بإساءة استخدام النظام لدوافع مختلفة، وتُشير الدراسات التي أجرتها دائرة المحاسبة العامة وشركة Orkand للاستشارات إلى أن الخسائر الناتجة عن جرائم الكمبيوتر تقدر بحدود 1.5 مليون دولار لشركات المصارف التي تستخدم الحاسب في الولايات المتحدة الأمريكية، ومن ناحية أخرى

(1) تمام، أحمد حسام طه، الجرائم الناشئة عن استخدام الحاسوب، (الحماية للحاسوب)، دراسة مقارنة، دار النهضة، القاهرة 2000م.

يقدر المركز الوطني لبيانات جرائم الحاسب في لوس أنجلوس بأن 70% من جرائم الكمبيوتر المسجلة حدثت من الداخل، أي من قبل مَن يعملون داخل المنظمات، هذا وأن جرائم الحاسب تزداد بصورة واضحة مما أصبحت تُشكّل تحدياً خطيراً يواجه الإدارات العليا عموماً وإدارة نظم المعلومات على وجه الخصوص[1].

وتُعتبر عملية الحماية من الأخطار التي تُهدد أنظمة المعلومات من المهام المعقدة والصعبة والتي تتطلب من إدارة نظم المعلومات الكثير من الوقت والجهد والموارد المالية، وذلك للأسباب التالية:

1 - العدد الكبير من الأخطار التي تُهدد عمل نظم المعلومات.

2 - توزع الوسائط الإلكترونية على العديد من المواقع التي يمكن أن تكون أيضاً متباعدة.

3 - وجود التجهيزات الرقمية في عهدة أفراد عديدين في المنظمة وأحياناً خارجها.

4 - صعوبة الحماية من الأخطار الناتجة عن ارتباط المنظمة بالشبكات الخارجية.

5 - التقدم التقني السريع يجعل الكثير من وسائل الحماية متقادمة من بعد فترة وجيزة من استخدامها.

6 - التأخر في اكتشاف الجرائم الرقمية مما لا يتيح للمنظمة إمكانية التعلم من التجربة والخبرة المتاحة[2].

7 - تكاليف الحماية يمكن أن تكون عالية بحيث لا تستطيع العديد من المنظمات تحملها.

---

(1) عرب، يونس، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، المرجع السابق.

(2) هلال، محمد رضوان، المحكمة الرقمية، المرجع السابق.

هذا وتقع مسئولية وضع خطة الحماية للأنشطة الرئيسية على مدير نظم المعلومات في المنظمة على أن تتضمن هذه الخطة إدخال وسائل الرقابة التي تضمن تحقيق ما يلي:

1 - الوقاية من الأخطار غير المتعمدة.

2 - إعاقة أو صنع الأعمال التخريبية المتعمدة.

3 - اكتشاف المشاكل بشكل مبكّر قدر الإمكان.

4 - المساعدة في تصحيح الأعطال واسترجاع النظام.

ويمكن تصميم نظام الرقابة ضمن عملية تطوير نظام المعلومات.ويجب أن يُركز هذا النظام على مفهوم الوقاية من الأخطار، ويمكن أن يصمم لحماية جميع مكونات النظام بما فيها التجهيزات.والبرمجيات والشبكات.

المطلب الثاني

اتجاهات الفقه حول تصنيف ظاهرة جرائم المعلوماتية

ثمة اتجاهات عدة حول تصنيف ظاهرة جرائم المعلوماتية انقسمت إلى الآراء الآتية:

الأول: اتجاه لا يرى إسباغ أية صفة إجرامية على هذه الفئة، أو على الأفعال التي تقوم بها، ولا يري وجوب تصنيفهم ضمن الطوائف الإجرامية لمجرمي الحواسيب، استناداً إلى أن صغار السن (المتلعثمين) «لديهم ببساطة ميل للمغامرة والتحدي، والرغبة في الاكتشاف، ونادراً ما تكون أهداف

أفعالهم المحظورة غير شرعية، واستناداً إلى أنهم لا يدركون ولا يقدرون مطلقاً النتائج المحتملة التي يمكن أن تؤدي إليها أفعالهم غير المشروعة بالنسبة لنشاط منشأة أو شركة تجارية»[1].

الثاني: الاتجاه الذي يحتفي بهذه الفئة ويُناصرها ويعتبرها ممن يُقدم خدمة لأمن المعلومات، ووسائل الحماية ويصفهم بالأخيار، وأحياناً بالإبطال الشعبيين ويتمادى هذا الاتجاه في تقديره لهذه الفئة بالمطالبة بمكافئتهم باعتبارهم لا يسببون ضرراً للنظام، ولا يقومون بأعمال احتيال، وينسب إليهم الفضل في كشف الثغرات الأمنية في تقنية المعلومات». ومثل هذا الرأي قال به أحد اشهر المدافعين عن الهاكرز الصغار، هيوجو كورن وعكس أفكاره في مؤلفه - الدليل الجديد للمتلعثمين - وبسبب خطورة ما يشيعه (هيوجو كورن ول) تم منع مؤلفه المذكور من قبل مركز بوليس مدينة لندن الكبرى (سكوتلاندیارد)، غير أن هذا المنع كان له أثر في توسيع دائرة انتشار هذا الكتاب وتحقيق نسبة عالية جداً من المبيعات[2]. ويتمادى الإعلامي (ستيفن ليف) في الاحتفال بهذه الفئة، واصفاً إياهم بأبطال ثورة الحاسبات متحمساً لهذا الوصف إلى درجة إطلاقه عنواناً على مؤلفه الخاص بهذه الظاهرة، لا لموقف معاد من التقنية، بل لأنه يرى في دوافعهم الخيرة لا الشريرة، الموجهة لمالكي، الأموال لا المحتاجين، ما ينهض بوصفهم بالأبطال الشعبيين[3].

الثالث: اتجاه يرى أن مرتكبي جرائم الحاسب من هذه الطائفة، يصنفون ضمن مجرمي الحاسب كغيرهم دون تمييز استناداً إلى أن تحديد الحد الفاصل بين العبث في الحاسبات وبين الجريمة أمر عسير من جهة، ودونما أثر على

(1) سلامة، محمد عبد الله أبو بكر، جرائم الكومبيوتر والانترنت موسوعة جرائم المعلوماتية، منشأة المعارف، الإسكندرية، 2006م.

(2) Tom forester, Essential proplems to Hig-Tech Society First MIT Pres edition, Cambridge, Massachusetts, 1989, p 104.

(3) تمام، أحمد حسام طه، الجرائم الناشئة عن استخدام الحاسوب، (الحماية للحاسوب)، دراسة مقارنة، المرجع السابق.

وصف الفعل - قانوناً - من جهة أخرى، واستناداً إلى أن خطورة أفعالهم التي تتميز بانتهاك الأنظمة واختراق الحاسبات وتجاوز إجراءات الأمن، والتي تعد بحق من أكثر جرائم الحاسب تعقيداً من الوجهة التقنية، عوضاً عن مخاطرها المدمرة ويدعم صحة هذا الاتجاه، التخوفات التي يُثيرها أصحاب الاتجاه الأول ذاتهم، إذ يخشون من الخطر الذي يواجه هذه الطائفة، والمتمثل باحتمال الانزلاق من مجرد هاوٍ صغير لاقتراف الأفعال غير المشروعة، إلى محترف لأعمال السلب، هذا إلى جانب خطر آخر أعظم، يتمثّل في احتضان منظمات الإجرام ومجرمين غارقين في الإجرام لهؤلاء الشباب[1].

المطلب الثالث

تصنيف الجرائم المعلوماتية

ظهرت تصنيفات كثيرة للجرائم المعلوماتية فصنفت تبعاً لدور الكمبيوتر في الجريمة أو تصنيف الجرائم تبعاً لمساسها بالأشخاص والأموال.

الفرع الأول

تصنيف الجرائم تبعاً لدور الكمبيوتر في الجريمة المعلوماتية

1 - جرائم تستهدف الكمبيوتر وذلك للاستيلاء على المعلومات أو إتلافها.

2 - تصنيف الجرائم الإلكترونية حسب الاتفاقية الأوربية في عام 2001م، وهي الجرائم التي تستهدف عناصر السرية والسلامة وتضم:

---

(1) هلال، محمد رضوان، المحكمة الرقمية، المرجع السابق.

- الدخول غير المصرَّح به.
- الاعتراض غير القانوني.
- تدمير المعطيات.
- اعتراض النظم.

3 - جرائم ترتكب بواسطة الكمبيوتر كجرائم الاحتيال.

الفرع الثاني

الجرائم المرتبطة بالكمبيوتر

1 - التزوير المرتبط بالكمبيوتر.

2 - الجرائم المرتبطة بالمحتوى وتضم تبعاً لهذه الاتفاقية الجرائم المتعلّقة بالأفعال الإباحية واللاخلاقية.

ظهور كل هذه الأنواع من الجرائم والتصنيفات المختلفة دعى الحكومات والدول إلى سن القوانين التي تحكم هذه الجرائم.

3 - الاحتيال المرتبط بالكمبيوتر.

المطلب الرابع

خصائص الجرائم الإليكترونية

1 - عالمية الجريمة:

بمعنى أنها لا تعترف بالحدود الجغرافية للدول وحتى بين القارات، لأنه مع انتشار شبكة الاتصالات العالمية «الانترنت» أمكن ربط أعداد هائلة منم لا حصر لها من الحواسيب عبر العالم لهذه الشبكة، حيث يمكن أن يكون الجاني في بلد والمجني عليه في بلد آخر، وهكذا فالجرائم الإلكترونية تقع في أغلب الأحيان عبر حدود دولية كثيرة.

2 - صعبة الإثبات:

صعوبة متابعتها واكتشافها فهي لا تترك أثراً، فهي مجرَّد أرقام تتغير في السجلات، فمعظم الجرائم الإلكترونية تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها، تفتقر إلى الدليل المادي التقليدي كالبصمات مثلاً[1].

وتعود أسباب صعوبة إثباتها إلى أن متابعتها واكتشافها من الصعوبة بمكان، حيث أنها لا تترك أثراً، فما هي إلا أرقام تدور في السجلات، كما أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف عنها، وتعود الصعوبة لأسباب:

1 - أنها كجريمة لا تترك أثراً بعد ارتكابها.

2 - صعوبة الاحتفاظ الفني بآثارها إن وجدت.

3 - أنها تحتاج لخبرة فنية يصعب على المحقق التقليدي التعامل معها.

4 - أنها تعتمد على الخداع في ارتكابها والتضليل في التعرُّف على مرتكبيها.

5 - أنها تعتمد على قمة الذكاء في ارتكابها[2].

3 - جرائم سهلة الوقوع:

إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي في ارتكابها كالقتل، السرقة، الاغتصاب، فالجرائم الإلكترونية لا تحتاج أدنى مجهود عضلي بل تعتمد عل الدراسة الذهنية، والتفكير العلمي المدروس القائم عن معرفة تقنية بالحاسب الآلي.

---

(1) رستم هشام الجرائم المعلوماتية، أصول التحقيق الجنائي الفني مجلة الأمن والقانون، دبي العدد (2)، 1999م.

(2) عبد الفتاح مراد، شرح جرائم الكمبيوتر والانترنت، دار الكتب والوثائق المصرية، ص 42.

المطلب الخامس

خصائص الجناة في جرائم الكمبيوتر والانترنت

لكي نستطيع فهم الجاني في الجرائم المعلوماتية الإلكترونية لابد من أن يوضع في الحسبان شخصية المجرم والذي ينبغي إعادة تأهيله اجتماعياً حتى يعود مواطناً صالحاً، ويمكننا القول أن الجاني في جرائم الحاسب الآلي يتمتع بقدر كبير من الذكاء علاوة على أنه إنسان اجتماعي بطبيعته:

أ - يتمتع الجاني في جرائم الإلكترونية بالذكاء:

بالإضافة إلى انتماء الجاني في جرائم الحاسب الآلي والتقنية إلى التخصصات المتصلة بعلومه من الناحية الوظيفية، يتمتع الجاني في هذه الجرائم بنظرة غير تقليدية له على اعتبار أنه يوصف غالباً بدرجة عالية من الذكاء المعلوماتي، تجعل من الصعب تصنيفه بحسب التصنيف الإجرامي المعتاد لذا ينظر في تحديد أنواع الجناة في الجرائم الإلكترونية إلى الهدف من ارتكابه لهذه الجرائم كمعيار للتميز فيما بينهم.

ب - الجاني في الجرائم الإلكترونية كإنسان اجتماعي:

الجاني في الجرائم الإلكترونية هو إنسان متوافق مع المجتمع حيث أنه إنسان شديد الذكاء يساعده على عملية التكيف مع هذا المجتمع. ولكنه يقترف هذا النوع من الجرائم بدافع اللهو أو لمجرد إظهار تفوقه على آلة الكمبيوتر أو على البرامج التي يتم تشغيله بها[1].

(1) تمام أحمد حسام طه، الجرائم الناشئة عن استخدام الحاسوب، (الحماية للحاسوب)، دراسة مقارنة، المرجع السابق.

المطلب السادس

الصعوبات تواجه مكافحة الجرائم المعلوماتية

1 - صعوبة التوصل إلى الأدلة الرقمية والتحفظ عليها.

2 - القصور التشريعي في تعريف مفهوم الجريمة الإلكترونية.

3 - عدم وجود مفهوم قانوني دولي مشترك لتعريف الجريمة الإلكترونية.

4 - قصور النصوص التشريعية الخاصة بمواجهة تلك الجرائم.

5 - قصور التعاون الدولي بين الدول في مجالات المكافحة.

المبحث السابع

طوائف المجرمون الرقميون

المطلب الأوَّل

طائفة المخترقون

وهذه الطائفة لا تختلف عن طائفة الهاكرز، علماً بأن بين الاصطلاحين تبايناً جوهرياً، فالهاكرز متطفلون يتحدُّون إجراءات أمن النظم والشبكات، لكن لا تتوافر لديهم في الغالب دوافع حاقدة أو تخريبية وإنما ينطلقون من دوافع التحدي وإثبات المقدرة، أما الكراكرز، فإن اعتداءاتهم تعكس ميولاً جريمة خطرة تنبيء عنها رغباتهم في إحداث التخريب، ومع أن هذا المعيار غير منضبط، إلا أن الدراسات القانونية في حقل جرائم الكمبيوتر والانترنت في الولايات المتحدة الأمريكية تعتمد هذا التمييز، فاصطلاح الكراكرز مرادف للهجمات الحاقدة والمؤذية في حين أن اصطلاح الهاكرز مرادف في الغالب لهجمات التحدي طبعاً دون أن يؤثر هذا التمييز على مسئولية مرتكبي الأنشطة من كلا الطائفتين ومساءلتهم عما يلحقونه من إضرار بالمواقع المستهدفة باعتداءاتهم[1].

وإن كان الاصطلاحين يختلفان واقعياً ومن حيث الأساس التاريخي لنشأة كل منهما. وأفراد هذه الطائفة يرتكبون جرائم التقنية بدافع التحدي الإبداعي ويجدون أنفسهم متفقين إلى درجة إلى أنهم ينصبون أنفسهم

(1) سلامة، محمد عبد الله أبو بكر، جرائم الكومبيوتر والانترنت موسوعة جرائم المعلوماتية، المرجع السابق.

أوصياء على أمن نظم الكمبيوتر في المؤسسات المختلفة، والسمة الغالبة على أعضاء هذه الطائفة صغر السن وقلة الخبرة وعدم التمييز بين الأنظمة محل الاختراق[1]، وبرغم هذه السمات فقد تمكن المجرمون من هذه الطائفة من اختراق مختلف أنواع نظم الكمبيوتر التابعة للشركات المالية والتقنية والبنوك ومصانع الألعاب والمؤسسات الحكومية ومؤسسات الخدمة العامة وكثر الحديث عن وقائع عملية كما في حالة اختراق أحد الصبية الذي يبلغ من العمر 14 عاماً نظام الكمبيوتر العائد للبنتاغون والأخر لا يتجاوز عمره السابعة عشرة تمكن من اختراق كمبيوترات العديد من المؤسسات الاستراتيجية في أوروبا والولايات المتحدة ومن بينها الكمبيوترات المتصلة ببرنامج حرب النجوم الذي كان مخطط لتنفيذه من قبل الولايات المتحدة في حقبة الحرب الباردة. والسمة المميزة الأخرى لهذه الطائفة تبادلهم للمعلومات فيما بينهم وتحديداً التشارك في وسائل الاختراق واليات نجاحها وإطلاعهم بعضهم البعض على مواطن الضعف في نظم الكمبيوتر والشبكات، حيث تجري عمليات التبادل للمعلومات فيما بينهم وبشكل رئيسي عن طريق النشرات الإعلامية الإلكترونية ومجموعات الأخبار، وفي تطور حديث لتنظيم هذه الطائفة نفسها يجري عقد مؤتمرات لمخترقي الكمبيوتر يدعى له الخبراء من بينهم للتشاور حول وسائل الاختراق ووسائل تنظيم عملهم فيما بينهم وبالرغم من أن الخطورة في هؤلاء تكمن بمثابرتهم على أنشطة الاختراق وتطوير معارفهم التقنية وبالرغم من توفر فرصة استغلال هؤلاء من قبل منظمات وهيئات إجرامية تسعى للكسب المادي، فإنه ومن ناحية أخرى ساهم العديد من هؤلاء المخترقين في تطوير نظم الأمن في عشرات المؤسسات في القطاعين الخاص والعام، حتى أن العديد من الجهات تستعين بخبراتهم في أحيان كثيرة في فحص وتدقيق مستوى أمن نظم الكمبيوتر والمعلومات[2].

---

(1) قايد، أسامة عبد الله، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، 1994 م.

(2) الحميد، محمد دباس، وماركوا ابراهيم نينو، حماية أنظمة المعلومات، دار الحامد، الطبعة

ونجد خلط في المواد التي تتناقلها الصحف والمجلات الوسائل الإعلامية - بين مجرمي التقنية وبين الهاكرز، وقد وصل الخلط إلى حد اعتبار كل مَن ارتكب فعلاً من أفعال الاعتداء المتصلة بجرائم الكمبيوتر والانترنت من قبيل الهاكرز، ربما لأن غالبية الاعتداءات تتم عن طريق الدخول غير المصرح به عبر شبكات المعلومات وتحديداً الانترنت، لكن الحقيقة غير ذلك، حتى أن هناك مَن يدافع عن مجموعات الهاكرز التي لا تمارس أية أفعال تستهدف إلحاق الضرر بالغير انطلاقاً إلى أن أغراض الاختراق لديهم تنحصر في الكشف عن الثغرات الأمنية في النظام محل الاعتداء، وثمة من يؤكد من بين الهاكرز المحترفين أن لديهم ضوابط وأخلاقيات خاصة بهم، بل أن العديد من مواقع الانترنت التي تهتم بمسائل الهاكرز أنشأها بعضهم ويعرضون فيها لمواد تتصل بتوضيح حقيقة هؤلاء ومحاولة سلخ أية صفة غير مشروعة أو إجرامية عن الأنشطة التي يقومون بها. ومع ذلك فإن علينا أن نقر بخطورة الهاكرز الذين تربوا في أجواء تحديات الاختراق والتفاخر بإبداعاتهم في هذا المجال والذين يتم استغلالهم من قبل مجموعات الجريمة المنظمة لارتكاب أفعال مخططة لها، فعنصر التحدي القائم لديهم لا يترك لديهم وازعاً للتراجع ولا يتيح لهم التمييز أو تقليب الأمور، وليس لديهم ضوابط بشأن النشاط الذي يقومون به النظام الذي يخترقونه[1].

ومجرموا الانترنت المحترفون تتميز هذه الطائفة بسعة الخبرة والإدراك الواسع للمهارات التقنية، كما تتميز بالتنظيم والتخطيط للأنشطة التي تُرتكب من قِبل أفرادها، ولذلك فإن هذه الطائفة تُعد الأخطر من بين مجرمي التقنية حيث تهدف اعتداءاتهم بالأساس إلى تحقيق بالكسب المادي لهم أو للجهات التي كلفتهم وسخرتهم لارتكاب جرائم الكمبيوتر كما تهدف اعتداءات بعضهم إلى تحقيق أغراض سياسية والتعبير عن موقف فكري أو نظري أو فلسفي. ويتم تصنيف أفراد هذه الطائفة إلى مجموعات متعددة إما تبعاً لتخصصهم بنوع معين من الجرائم أو تبعاً للوسيلة المتبعة من قبلهم في ارتكاب الجرائم فمثلاً نجد طائفة محترفي التجسس الصناعي وهم أولئك

الأولى، سنة 2007م.

(1) Edward Waltz, Information Warfare Principles and Operations, 1998.

الذين يوجهون أنشطهم إلى اختراق نظم الكمبيوتر العائدة للشركات الصناعية ومشاريع الأعمال بقصد الاستيلاء على الأسرار الصناعية والتجارية إما لحساب أعمال يقومون بها بذاتهم أو في الغالب لحساب منافسين آخرين في السوق، وأحياناً لحساب مجموعات القرصنة الدولية. ونجد مثلاً طائفة مجرمي الاحتيال والتزوير، وهؤلاء هم الطائفة التي تكون أغراضها متجهة إلى تحقيق كسب مادي والاستيلاء على أموال الآخرين وضمن هذه الطائفة أيضاً ثمة تصنيفات عديدة فمنهم محتالوا شبكات الهاتف محتالو الانترنت وغير ذلك، وحتى في الطائفة الفرعية[1]، قد تتوفر تخصصات لبعضهم كأن يوجه الشخص أنشطته الاحتيالية إلى قطاع مزادات البضاعة والمنتجات على الانترنت أو في ميدان الاستيلاء على أرقام بطاقات الائتمان والاتجار بها. والى جانب المعرفة التقنية المميزة والتنظيم العالي والتخطيط للأنشطة المنوي ارتكابها، فإن أفراد هذه الطائفة يتسمون بالتكتم خلافاً للطائفة الأولى فلا يتبادلون المعلومات بشأن أنشطتهم بل يطورون معارفهم الخاصة ويحاولون ما أمكن عدم كشف طرقهم التقنية لارتكاب جرائمهم وحول الأعمار الغالبة على هذه الطائفة فان الدراسات تشير إلى أنهم من الشباب الأكبر سناً من الطائفة الأولى وأن معظمهم تتراوح أعمارهم ما بين 25 - 40 عام[2].

المطلب الثاني

طائفة المحترفون

وهم المجرمون البالغون أي محترفو الإجرام أن مرتكبي جرائم الحاسب، وينتمون وفق لعدة دراسات إلى فئة عمرية تتراوح بين (25 - 45) عاماً، وبالتالي، يمتاز مرتكبوا هذه الجرائم بصفات الشباب العمرية والاجتماعية، وإذا استثنينا صغار السن من بينهم، الذين تكون أعمارهم دون الحد الأدنى المشار إليه أعلاه، كما رأينا فيما سلف، فإن لمجرمي الحاسب سمات عامة،

(1) هلال، محمد رضوان، المحكمة الرقمية، المرجع السابق.

(2) رون وايت، كيف تعمل الحواسيب، ترجمة ونشر الدار العربية للمعرفة والعلوم، بيروت 1999م.

يتحقق بعضها لدرجة أقل في صغار السن وهذه السمات أما عن الصفات الشخصية والتخصص والكفاءة لتلك الطائفة فإن الجامع بين محترفي جرائم الحاسب، تمتعهم بقدرة عالية من الذكاء، وإلمام جيد بالتقنية العالية، واكتسابهم معارف عملية وعلمية، وانتمائهم إلى التخصصات المتصلة بالحاسب من الناحية الوظيفية، وهذه السمات تتشابه مع سمات مجرمي ذوي الياقات البيضاء»[1] أما فيما يتعلّق بكفاءة مجرمي الحاسب، فإن الدراسات القليلة المتوفرة، تُشير إلى تمتعهم بكفاءة عالية، إلى درجة اعتبارهم مستخدمين مثاليين من قِبل الجهات العاملين لديها، وممَّن يوسمون بالنشاط الواسع والإنتاجية الفاعلة، والجوانب السيكولوجية لهذه الطائفة أن الدراسات القليلة للجوانب السيكولوجية لمجرمي الحاسب، أظهرت شيوع عدم الشعور بلا مشروعية الطبيعة الإجرامية وبلا مشروعية الأفعال التي يقارفونها، كذلك الشعور بعدم استحقاقهم للعقاب عن هذه الأفعال، فحدود الشر والخير متداخلة لدى هذه الفئة، وتغيب في وداخلهم مشاعر الإحساس بالذنب، وهذه المشاعر في الحقيقة تبدو متعارضة مع ما تظهره الدراسات من خشية مرتكبي جرائم الحاسب من اكتشافهم وافتضاح أمرهم، ولكن هذه الرهبة والخشية يُفسرها انتماؤهم في الأعم الأغلب إلى فئة اجتماعية متعلمة ومثقفة[2].

والحاقدون من هذه الطائفة يغلب عليها عدم توفر أهداف الجريمة المتوفرة لدى الطائفتين السابقتين، فهم لا يسعون إلى إثبات المقدرات التقنية والمهارية وبنفس الوقت لا يسعون إلى مكاسب مادية أو سياسية، إنما يُحرك أنشطتهم الرغبة بالانتقام والثأر كأثر لتصرُّف صاحب العمل معهم أو لتصرُّف المنشأة المعنية معهم عندما لا يكونوا موظفين فيها، ولهذا فإنهم ينقسمون أما إلى مستخدمي للنظام بوصفهم موظفين، أو مشتركين، أو على علاقة ما

---

(1) عبد المطلب، ممدوح عبد الحميد، جرائم استخدام شبكة المعلومات العالمية (الجريمة عبر الانترنت)، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، بجامعة الإمارات العربية المتحدة، عام 2000م.

(2) عرب، يونس، جرائم الكمبيوتر والانترنت، موسوعة القانون وتقنية المعلومات، منشورات اتحاد المصارف العربية، الطبعة الأولى، الجزء الثاني، 2002م.

بالنظام محل الجريمة، وإلى غرباء عن النظام تتوفر لديهم أسباب الانتقام من المنشأة المستهدفة في نشاطهم. ولا يتّسم أعضاء هذه الطائفة بالمعرفة التقنية الاحترافية، ومع ذلك يشقى الواحد منهم في الوصول إلى كافة عناصر المعرفة المتعلّقة بالفعل المخصوص الذي ينوي ارتكابه، وتغلب على أنشطتهم من الناحية التقنية استخدام تقنيات زراعة الفيروسات والبرامج الضارة، وتخريب النظام، أو إتلاف كل أو بعض معطياته، أو نشاط إنكار الخدمة وتعطيل النظام أو الموقع المستهدَف إن كان من مواقع الانترنت. وليس هناك ضوابط محدَّدة بشأن أعمارهم، كما أنه لا تتوفر عناصر التفاعل بين أعضاء هذه الطائفة، ولا يفاخرون بأنشطتهم بل يعمدون إلى إخفائها، وهم الطائفة الأسهل من حيث كشف الأنشطة التي قاموا بارتكابها لتوفر ظروف وعوامل تساعد في ذلك. وبالرغم من أن سمات هذه الطائفة تضعها من حيث الخطورة في مؤخرة الطوائف المتقدمة إذ هم أقل خطورة من غيرهم من مجرمي التقنية، لكن ذلك لا يمنع أن تكوّن الأضرار التي نجمت عن أنشطة بعضهم جسيمة ألحقت خسائر فادحة بالمؤسّسات المستهدفة[1].

المطلب الثالث

طائفة صغار السن

تتّصف هذه الطائفة بأنهم «الشباب البالغ المفتون بالمعلوماتية والحاسبات الآلية»[2] فإن من بينهم في الحقيقة، فئة لما تزل دون سن الأهلية مولعين بالحاسبات والانترنت. وقد تعددت أوصافهم في كثير من الدراسات

---

(1) عرب، يونس، جرائم الكمبيوتر والانترنت، موسوعة القانون وتقنية المعلومات، المرجع السابق.

(2) الطويل، خالد بن محمد، التعامل مع الاعتداءات الإلكترونية من الناحية الأمنية مركز المعلومات الوطني، وزارة الداخلية، ورقة عمل مقدمة لورشة العمل الثالثة (أحكام في المعلوماتية) الذي نظمه مشروع الخطة الوطنية لتقنية المعلومات 1423/10/19هـ الرياض.

وشاع في نطاق الدراسات الإعلامية والتقنية، حسب تعبير الأستاذ توم فور ستر، على «الصغار المتحمسين للحاسبات، بشعور من البهجة، دافعهم التحدي لكسر الرموز السرية لتركيبات الحاسب»[1] ويسميهم البعض كذلك بمجانين (معدلات ومعدلات عكسية) بالاستناد إلى كثرة استخدامهم لتقنية (الموديم)، الذي يعتمد على الاتصال الهاتفي لاختراق شبكة النظم - ويثير مجرمو الحاسبات من هذه الطائفة جدلاً واسعاً، ففي الوقت الذي كثر الحديث فيه عن مخاطر هذه الفئة، على الأقل بمواصلتها العبث بالحاسبات، وظهرت كثير من الدراسات تدافع عن هذه الفئة، لتخرجها من دائرة الإجرام إلى دائرة العبث[2].

ومن الأمثلة الشهيرة لجرائم الحاسب التي ارتكبت من هذه الفئة، العصابة الشهيرة التي أطلق عليها (عصابة 414) والتي نسب إليها ارتكاب ستون فعل تُعد في الولايات المتحدة الأمريكية على ذاكرات الحاسبات، نجم عنها أضرار كبيرة لحقت بالمنشآت العامة والخاصة. وكذلك، تلاميذ المدرسة الثانوية في ولاية (منهاتن) الذين استخدموا في عام (1980) طرفيات غرف الدرس للدخول إلى شبكة اتصالات وبيانات كثير من المستخدمين ودمروا ملفات زبائن الشركة الرئيسية في هذه العملية. كما سبب متلعثمو ألمانيا الغربية الصغار في عام 1984 م فوضى شاملة، عندما دخلوا إلى شبكة (الفيديو تكس) ونجح بعض المتلعثمون الفرنسيون في إيجاد مدخل إلى الملفات السرية لبرنامج ذري فرنسي[3]. ويمكن رد الاتجاهات التقديرية لطبيعة هذه الفئة، وسمات أفرادها، ومدى خطورتهم.

---

(1) هلال، محمد رضوان، المحكمة الرقمية، المرجع السابق.

(2) سلامة، محمد عبد الله أبو بكر، جرائم الكومبيوتر والانترنت موسوعة جرائم المعلوماتية، المرجع السابق.

(3) Spreutels (J.P.): Les crimes informatiques ET d'autres crimes dans le domaine de la technologie informatique en Belgique, Rev. Int. dr. pen. 1993. p 161.

المبحث الثامن

التنظيم التشريعي للوثائق الإليكترونية

استجابت العديد من دول العالم إلى الاتجاه السابق واعترفت بحجية المستندات الإليكترونية في الإثبات ومن ثم إلى اعتبارها محلاً لجريمة التزوير وقد كانت المملكة الأردنية سباقة في ذلك؛ حيث أصدرت قانون الأوراق المالية المؤقت رقم 23 لسنة 1997 م الذي نص في المادة 2/24 على أن تعتبر القيود المدونة في سجلات البورصة وحساباتها سواء كانت مدونة يدوياً أو إلكترونياً، أو أي وثائق صادرة عنها دليلاً على تداول الأوراق[1].

أما بالنسبة لتجريم تزوير الوثائق الإليكترونية، فقد كان القانون الفرنسي رقم 19 الصادر في يناير 1988 م أولى التشريعات التي جرَّمت تزوير المستندات المعلوماتي فنص في المادة 5/462 على أن «كل مَن ارتكب أفعالاً تؤدي إلى تزوير المستندات المعلوماتية أياً كان شكلها بأي طريقة تؤدي إلى حدوث ضرر للغير فإنه يُعاقب بالسجن من سنة إلى خمس سنوات وغرامة لا تقل عن 20.000 فرنك»، ونصت الفقرة السادسة من ذات المادة على معاقبة كل مَن استخدم بتبصير المستندات المعلوماتية المزورة طبقاً للفقرة السابقة، ولم يكتفِ المشرِّع الفرنسي بذلك بل إنه نص على إمكانية ارتكاب جريمة التزوير خطأ؛ لأن التغيير والتحريف للمعلومات المخزنة خطأ وإن كان غير متصور في المستندات والوثائق التقليدية إلا أنه كثيراً ما يحدث في المجالات المعلوماتية؛ لأن الدخول إلى الأنظمة المعلوماتية لا يحدث دائماً بشكل متعمد فمن الممكن أن يحدث بشكل غير معتمد نتيجة الدخول الخاطئ

(1) عرب، يونس، جرائم الكمبيوتر والانترنت، موسوعة القانون وتقنية المعلومات، المرجع السابق.

إليه وهو ما يجب النص عليه في تجريم التزوير في المستندات المعلوماتية.

وكل حالات السرقة والاحتيال تتم عن طريق تزوير البيانات وهي حالة من حالات تعدد الجرائم سواء كانت السرقة بتصميم برنامج معد خصيصاً أو عن طريق إجراء عمليات تحويل غير مشروعة للأرصدة بخلق حسابات دائنة وهمية كلها لا تتم إلا بتزوير في البيانات المخزنة آلياً لنجد أن معظم الحالات يتحقّق فيها التعدد المعنوي للجرائم خاصة مثل التلاعب الذي يتم في الأرصدة المصرفية؛ لأن عمليات التحويل غير المشروعة تتم عن طريق تعديل في البيانات والأسماء، أو تعديل في البرامج المعلوماتية المعالجة لهذه البيانات، فإذا كان السلوك الإجرامي في هذه الحالة متمثلاً في تعديل البرامج والبيانات يترتب عليه تحويلات مالية غير مشروعة، فإن السلوك أو الفعل يظل واحداً يتحقّق به أكثر من نموذج تجريمي في هذه الحالة وهو ما يوجب تطبيق أحكام التعدد المعنوي والارتباط بين الجرائم[1].

وتجدر الإشارة إلى أن هذا التوسّع في تفسير مفهوم الوثيقة لا يغني عن ضرورة تدخل المشرّع لمواجهة التزوير المرتكب بالحاسب الآلي على المستندات والوثائق الإليكترونية، لأن المساءلة تحتاج أولاً إلى الاعتراف بحجية هذه المستندات الإليكترونية في الإثبات قبل تجريم تحريفها، بالإضافة إلى أن تجريم التعديل في هذه البيانات يجب أن يخضع لعقوبات أشد من عقوبة التزوير التقليدية نظراً لاختلاف حجم الضرر والخسائر الناتجة عن تحريف هذه البيانات وتزويرها[2].

وقد نصت اتفاقية بودابست في المادة 7 على تجريم أي تبديل، أو محو، أو إخماد لأي بيانات مخزّنة في أي نظام معلوماتي يؤدي إلى إنتاج بيانات غير حقيقة لغرض استعمالها لأغراض قانونية على أنها صحيحة وذلك سواء

(1) راجع الرابط http://lahmawy. own0. com/t1463-topic

(2) تمام، أحمد حسام طه، الجرائم الناشئة عن استخدام الحاسوب، (الحماية للحاسوب)، دراسة مقارنة، المرجع السابق.

كانت فورية القراءة من عدمها وهو ما يقطع الجدل حول قابلية المستند للقراءة بالعين المجردة، واعتبار المستند الإليكتروني وثيقة قابلة للقراءة، مشمولة بالحماية الجنائية[1].

يتضح لنا أن الجريمة المعلوماتية تُثير مشكلات عديدة في تطبيق النصوص القانونية الحالية، فإن وجد النص القانوني وأمكن أعمال المطابقة بينه وبين السلوك المرتكب لا نجد العقوبة تتناسب وحجم الخسائر الناتجة عن ارتكاب مثل هذه الجريمة، وإذا أمكن أعمال المطابقة وكانت العقوبة رادعة فإننا نواجه عقبة كبيرة في عمليات ضبط هذه الجرائم وإثباتها لأن القواعد التقليدية للإثبات وضعت لتواجه سلوكاً مادياً يحدث في العالم الحالي، لا تتناسب لإثبات جريمة مرتكبة في عالم إليكتروني، أو فضاء سيبراني افتراضي غير ملموس يتكون من ذبذبات والموجات غير المرئية. وهو ما يُحتم ضرورة التدخل التشريعي لتنظيم هذه المسألة عن طريق الاعتراف لقوة المستندات الإلكتروني في الإثبات، واعتبارها من قبيل الوثائق قبل النص على تجريم تزويرها أو التعديل فيها وتحريفها حسب الأحوال[2].

---

(1) خميس، فوزي، جرائم المعلوماتية وحماية الملكية المعلوماتية وبنوك وقواعد المعلومات، محاضرة القيت في نقابة المحامين في بيروت بتاريخ 1999/2/25م.

(2) راجع الرابط http://lahmawy. own0. com/t1463-topic

المبحث التاسع

التكييف القانوني والأبعاد الفنية للجرائم المعلوماتية

المطلب الأول

التكييف القانوني للجرائم المعلوماتية

لقد تدخل القانون العربي النموذجي بالنص مع تجريم الصور السابقة والاستيلاء على الأموال فنص في المادة 6 على أنه« كل مَن استخدم بطاقة ائتمانية للسحب الإلكتروني من الرصيد خارج حدود رصيده الفعلي أو باستخدام بطاقة مسروقة أو تحصل عليها بأية وسيلة بغير حق أو استخدام أرقامها في السحب أو الشراء وغيرها من العملات المالية مع العلم بذلك وهو ما يعني أن هذا النص قاصراً على توفير الحماية لغيرها من البطاقات لتقدير الدولة».

أما اتفاقية بودابست السابق الإشارة إليها فقد نصت المادة 8 منها والخاصة بالتحايل المرتبط بالحاسب computer related frau على معاقبة أي شخص يتسبب بأي خسائر مادية للغير عن طريق تعديل أو محو أو إيقاف لأي بيانات مخزَّنة في أي نظام معلوماتي أو عن طريق أي تدخل فيه، وبذلك تتوفر الحماية الجنائية اللازمة للأموال في مواجهة السلوك المرتكب بالحاسب الآلي[1].

---

(1) عرب، يونس، جرائم الكمبيوتر والانترنت، موسوعة القانون وتقنية المعلومات، المرجع السابق

إذا كانت جرائم الأموال المرتكبة بواسطة الحاسب الآلي تواجه فراغاً تشريعياً في ليبيا، فإن المشكلة الحقيقة في نظرنا بالنسبة لهذه الجرائم لا تتمثّل في الفراغ التشريعي بقدر ما هي كامنة في طرق ضبطها وإثباتها، وهو ما يرجع إلى افتقاد الآثار التقليدية التي قد تتركها أي جريمة في الجريمة المعلوماتية، فالبيانات يتم إدخالها مباشرة في الجهاز دون أن تتوقف على وجود وثائق أو مستندات؛ لأنه كثيراً ما يكون هناك برامج معدة ومخزّنة سلفاً على الجهاز ولا يكون عليه سوى إدخال البيانات في الأماكن المعدة لها كما هو الحال بالنسبة للمعاملات المصرفية والمؤسسات التجارية الكبرى، ويمكن في هذه الفروض اقتراف جرائم الاختلاس والتزوير فتفقد الجريمة آثارها التقليدية[1]. فالجريمة المعلوماتية تُرتكب في مسرح خاص هو يتمثّل في عالم افتراضي مفرغ cyberspace وهو ما يختلف كلياً عن المسرح الذي تُرتكب فيه الجرائم في صورتها التقليدية؛ حيث تُطبق القواعد العامة لانتداب الخبراء في اقتفاء آثار الجناة، الذين يرتكبون جرائم تتكون من سلوك مادي ملموس وله محل مادي ملموس أيضاً، مما لا يتناسب ونوع الخبرة المطلوبة لمعاينة المسرح السيبيري للجريمة المعلوماتية المرتكبة في الفضاء الإلكتروني.

فالخبرة المطلوبة للتحقيق في الجريمة المعلوماتية يجب أن تكون على درجة عالية من الكفاءة العلمية أو العملية أيضاً، وهو ما يوجب أن يكون الخبير في الجريمة المعلوماتية ملماً بأدق تفاصيل تركيب الحاسب وعمل الشبكات المعلوماتية والأماكن المحتملة للأدلة كالمواضع التي يمكن أن تحتفظ بآثار الاختراق وتوقيته، والبرامج المستخدمة في أي عملية تمت أثناء الاختراق، بالإضافة إلى إمكانية نقل الأدلة إلى أوعية أخرى دون تلف[2].

يجب الإشارة أيضاً إلى أن ملاحقة الجرائم المعلوماتية لا يتطلب رفع

(1) بيومي، حجازي عبد الفتاح، جرائم الكمبيوتر والانترنت، دار الكتب القانونية، القاهرة، 2005م.

(2) عرب، يونس، جرائم الكمبيوتر والانترنت، موسوعة القانون وتقنية المعلومات، المرجع السابق

كفاءة الخبراء فقط، بل أنها تحتاج إلى رفع كفاءة مأموري الضبط القضائي بصفة عامة؛ لأن مأمور الضبط القضائي أول شخص يكتشف الجريمة ويتصل بمسرحها والمسئول الأول عن التحفظ على أي أثر يتركه الجاني بعد ارتكابه للجريمة، مما يستوجب أن يكون المتعامل الأول مع النظام المعلوماتي على درجة من الكفاءة تسمح له بالتحفظ على هذه الأدلة؛ لأن أي خطأ في التعامل الأولى مع هذه الأجهزة قد يؤدي إلى محو الأثر أو الأدلة[1].

أما اتفاقية بودابست السابق الإشارة إليها فقد أشارت في القسم الإجرائي منها في المادة 16 إلى أنه: (على الدول الأعضاء العمل على تطبيق أنظمة فنية لحماية البيانات المخزنة مع إلزام العاملين في أي نظام معلوماتي بحفظ كل العمليات المنطقية التي تجري على الأجهزة لمدة لا تقل على 90 يوماً)، وهو ما يعني أن الاتفاقية تشترط مستوى معيناً للكفاءة الفنية في العمل بهذه التقنية، مما يعني أننا نحتاج إلى برنامج وطني متكامل لرفع مستوى كفاءة العمل بهذه التقنية قبل الحديث عن إمكانية تطبيق هذه المعاهدة.

المطلب الثاني

الأبعاد الفنية للأفعال الجنائية المرتكبة

إن مواكبة القوانين الدولية والعربية والمحلية للجرائم المستحدثة ومنها جرائم الانترنت، ولكن ما هي المنطلقات الشرعية والقانونية لاطلاق مصطلح جريمة على الأفعال المرتكبة أثناء استخدام الانترنت في المجتمع السعودي. يمكن أن نقول أنه يستحسن التطرق بشيء من التفصيل للجرائم والأفعال التي تطرقت إليها الدراسة وتكيفها شرعياً وقانونياً وهذه الأفعال هي:

(1) سلامة، محمد عبد الله أبو بكر، جرائم الكومبيوتر والانترنت موسوعة جرائم المعلوماتية، المرجع السابق.

أولاً: الجرائم الجنسية والممارسات غير الأخلاقية وتشمل:

1 - المواقع والقوائم البريدية الإباحية: يندرج تحت هذا البند جرائم ارتياد المواقع الإباحية، الشراء منها، الاشتراك فيها، أو إنشائها، وقد «أصبح الانتشار الواسع للصور والأفلام الإباحية على شبكة الانترنت يُشكل قضية ذات اهتمام عالمي في الوقت الراهن، بسبب الازدياد الهائل في أعداد مستخدمي الانترنت حول العالم»[1] وتختلف المواقع الإباحية عن القوائم البريدية – التي تخصص لتبادل الصور والأفلام الجنسية – في أن المواقع الإباحية غالباً ما يكون الهدف منها الربح المادي حيث يستوجب على متصفح هذه المواقع دفع مبلغ مقطوع مقابل مشاهدة فيلم لوقت محدد أو دفع اشتراك شهري أو سنوي مقابل الاستفادة من خدمات هذه المواقع، وإن كانت بعض هذه المواقع تحاول استدراج مرتاديها بتقديم خدمة إرسال صور جنسية مجانية يومية على عناوينهم البريدية، كما أن تصفح الموقع يتطلب في الغالب الاتصال المباشر بشبكة الانترنت مما يعنى أنه قد يتم حجبه من قبل مدينة الملك عبد العزيز للعلوم والتكنولوجيا، فلا يمكن الوصول إليه إلا باستخدام البروكسي. أما القوائم البريدية فهي أسهل إنشاءً، وغالباً مجانية ويقوم أعضائها من المشتركين بتبادل الصور والأفلام على عناوينهم البريدية وربما تكون القوائم البريدية أبعد عن إمكانية المتابعة الأمنية حيث يركز نشاطها على الرسائل البريدية والتي تكون من الصعوبة بمكان منعها عن أعضاء أي مجموعة، حتى وإن تم الانتباه إلى تلك القائمة لاحقاً وتم حجبها، فإن الحجب يكون قاصراً على المشتركين الجدد واللذين لا يتوفر لديهم وسائل تجاوز المرشحات، أما الأعضاء السابقين فلا حاجة لهم إلى الدخول إلى موقع القائمة حيث يصل إلى بريدهم ما يردونه دون أن تستطيع

(1) الطويل، خالد بن محمد، التعامل مع الاعتداءات الإلكترونية من الناحية الأمنية مركز المعلومات الوطني، وزارة الداخلية، ورقة عمل مقدمة لورشة العمل الثالثة (أحكام في المعلوماتية) الذي نظمه مشروع الخطة الوطنية لتقنية المعلومات 1423/10/19هـ الرياض.

وسائل الحجب التدخل. ويشترك في القوائم البريدية آلاف الأشخاص التي تصل أي رسالة يرسلها مشترك منهم إلى جميع المشتركين مما يعني كم هائل من الرسائل والصور الجنسية التي يتبادلها مشتركي القائمة بشكل يومي. واستفادت هذه المواقع والقوائم من الانتشار الواسع للشبكة والمزايا الأخرى التي تقدمها حيث « تتيح شبكة الانترنت أفضل الوسائل لتوزيع الصور الفاضحة والأفلام الخليعة بشكل علني فاضح يقتحم على الجميع بيوتهم ومكاتبهم، فهناك على الشبكة طوفان هائل من هذه الصور والمقالات والأفلام الفاضحة بشكل لم يسبق له مثيل في التاريخ»[1]، فكل مستخدم للانترنت معرض للتأثر بما يتم عرضه على الانترنت الذي لا يعترف بأي حدود دولية أو جغرافية فهو يُشكل خطراً حقيقياً للأطفال فضلاً عن الكبار نتيجة تأثيراته المؤذية وغير المرغوبة[2]. ويوجد على الانترنت آلاف المواقع الإباحية وعدد كبير جداً من القوائم الجنسية والتي أصبحت أكثر تخصصاً، فهناك قوائم خاصة للشواذ من الجنسين، وهناك قوائم أخرى تصنف تحت دول محددة ومن المؤسف أنه وجدت بعض المواقع الشاذة بمسميات عربية بل وسعودية والأدهى والأمَرّ أن يربط بين بعض القوائم الإباحية والإسلام كموقع أسمى نفسه «السحاقيات المسلمات» وهكذا. وكشفت إحدى الدراسات أن معدل التدفق على الواقع الإباحية في أوقات العمل التي تبدأ من الساعة التاسعة صباحاً إلى الخامسة عصراً تمثل (70%) من إجمالي نسبة التدفق على تلك المواقع (بي بي سي، 2001م). كما كشفت دراسة قام بها أحد المتخصصين[3] بأن هناك إقبال كبير جداً على المواقع الإباحية حيث تزعم

(1) فايد، أسامة عبد الله، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، المرجع السابق.

(2) تمام أحمد حسام طه، الجرائم الناشئة عن استخدام الحاسوب، (الحماية للحاسوب)، دراسة مقارنة، المرجع السابق.

(3) الطويل، خالد بن محمد، التعامل مع الاعتداءات الإلكترونية من الناحية الأمنية مركز المعلومات الوطني، وزارة الداخلية، ورقة عمل مقدمة لورشة العمل الثالثة (احكام في المعلوماتية) الذي نظمه مشروع الخطة الوطنية لتقنية المعلومات 1423/10/19هـ.

شركة (Playboy) الإباحية بأن (4.7) مليون زائر يزور صفحاتهم على الشبكة أسبوعياً، وبأن بعض الصفحات الإباحية يزورها (280.034) زائر يومياً وأن هناك مائة صفحة مشابهة تستقبل أكثر من (20.000) ألف زائر يومياً وأكثر من ألفين صفحة مشابهة تستقبل أكثر من (1400) زائر يومياً، وأن صفحة واحدة من هذه الصفحات استقبلت خلال عامين عدد (43.613.508) مليون زائر، كما وجد أن (83.5%) من الصور المتداولة في المجموعات الإخبارية هي صور إباحية، وبأنّ أكثر من (20%) من سكان أمريكا يزورون الصفحات الإباحية حيث تبدأ الزيارة غالباً بفضول وتتطور إلى إدمان، وغالباً لا يتردد زوار هذه المواقع من دفع رسوم مالية لقاء تصفح المواد الإباحية بها أو شراء مواد خليعة منها وقد بلغت مجموعة مشتريات مواد الدعارة في الانترنت في عام (1999م) ما نسبته (8%) من دخل التجارة الإلكترونية البالغ (18) مليار دولار أمريكي في حين بلغت مجموعة الأموال المنفقة للدخول على المواقع الإباحية (970) مليون دولار ويتوقع ارتفاع المبلغ ليصل إلى (3) مليار دولار في عام (2003م)، وقد أتضح أن أكثر مستخدمي المواد الإباحية تتراوح أعمارهم ما بين (12) و(15) عام في حين تمثّل الصفحات الإباحية أكثر صفحات الانترنت بحثاً وطلباً. كما وضحت دراسة أكدت أن المواقع الإباحية أصبحت مشكلة حقيقة وأن الآثار المدمرة لهذه المواقع لا تقتصر على مجتمع دون الآخر، ويمكن أن يلمس آثارها السيئة على ارتفاع جرائم الاغتصاب بصفة عامة واغتصاب الأطفال بصفة خاصة، العنف الجنسي، فقد العائلة لقيمها ومبادئها وتغيير الشعور نحو النساء إلى الابتذال بدل الاحترام. ويبدوا أن لكثرة المواقع الإباحية على الانترنت والتي يُقدر عددها بحوالي (70.000) ألف موقع دور كبير في إدمان مستخدمي الانترنت عليها حيث أتضح أن نسبة (15%) من مستخدمي الانترنت البالغ عددهم (9.600.000) مليون شخص تصفحوا المواقع الإباحية في شهر ابريل عام (1998م). وقد جرى حصر القوائم العربية الإباحية فقط دون القوائم الأجنبية في بعض المواقع على

الرياض.

شبكة الانترنت، ومنها موقع الياهو (YAHOO) فوجد أنها تصل إلى (171) قائمة، بلغ عدد أعضاء أقل تلك القوائم (3) في حين وصل عدد أكثرها أعضاء إلى (8683) أما موقع قلوب لست (GLOBELIST) فقد احتوى على (6) قوائم إباحية عربية، في حين وجد عدد (5) قوائم عربية إباحية على موقع توبيكا (TOPICA) وقد قامت مدينة الملك عبد العزيز للعلوم والتقنية مشكورة بإغلاق تلك المواقع. فارتياد مثل هذه المواقع ومشاهدة المواد الجنسية بها من المحظورات الشرعية التي حرص الشارع الحكيم على التنبيه عليها وتحريمها، بل إن الشارع الحكيم أمرنا بغض البصر وحرّم النظر إلى الأجنبيات سواء بصورة أو حقيقة وليس فقط تجنُّب النظر إلى الحرام فقال عز وجل في كتابه الحكيم: ﴿قُل لِّلْمُؤْمِنِينَ يَغُضُّوا مِنْ أَبْصَارِهِمْ وَيَحْفَظُوا فُرُوجَهُمْ ذَلِكَ أَزْكَى لَهُمْ إِنَّ اللَّهَ خَبِيرٌ بِمَا يَصْنَعُونَ﴾[1]. فهناك ولا شك علاقة بين «ارتكاب الأفعال الجنسية المحرمة والنظر إلى الصور الجنسية العارية، فالدين الإسلامي الحنيف حذر من ظاهرة النظر للعراة، لما تحدثه من تصدعات أخلاقية في الفرد والمجتمع»[2] ويذهب الشارع إلى أبعد من ذلك لعلمه بمخاطر النظر وما يمكن أن يوصل إليه، فحرّم رسول الله صلى الله عليه وسلم أن تصف المرأة لزوجها جمال امرأة أخرى لا تحل له وكأنه ينظر إليها فقال عليه الصلاة والسلام في الحديث الذي رواه البخاري في صحيحه وأحمد في مسنده واللفظ للبخاري: «قَالَ النَّبِيُّ ﷺ لَا تُبَاشِرُ الْمَرْأَةُ الْمَرْأَةَ فَتَنْعَتَهَا لِزَوْجِهَا كَأَنَّهُ يَنْظُرُ إِلَيْهَا كل هذه الأمور اهتم بها الشارع وحرمها كونها موصلة لجريمة الزنا التي تعد من الكبائر والتي متى ما اجتنب الأفراد هذه الأفعال فلن يقعوا في الزنا. ولعل من حكمة الشارع ومعرفته بالغرائز البشرية التي يُساهم الشيطان في تأجيجها ليوقع الإنسان فيما

(1) سورة النور/الآية 30.

(2) القاسم، محمد بن عبد الله، والزهراني، رشيد، والسند، عبد الرحمن بن عبد الله، العمري، عاطف تجارب الدول في مجال أحكام في المعلوماتية، مشروع الخطة الوطنية لتقنية المعلومات، 1423هـ.

حرم الله، ولعظمة جريمة الزنا فإنه لم يحرم الزنا فقط بل حرم الاقتراب منه فقال تعالى: ﴿وَلَا تَقْرَبُوا الزِّنَى إِنَّهُ كَانَ فَاحِشَةً وَسَاءَ سَبِيلًا﴾[1]، يقول القرطبي رحمه الله في تفسير هذه الآية: «قال العلماء قوله تعالى: ﴿ولا تقربوا الزنى﴾ أبلغ من أن يقول ولا تزنوا، فإن معناه فلا تدنوا من الزنا. فأي اقتراب من المحظور هو فعل محظور في حد ذاته، ومن ذلك مشاهدة المواد الجنسية فضلاً عن الاشتراك في تلك القوائم الإباحية أو شراء مواد جنسية منها أو، وهو الأخطر ضرراً: إنشائها كون الفعل الأخير متعدي ضرره للغير ويدخل فاعله في وعيد الله عز وجل حين قال: ﴿إِنَّ الَّذِينَ يُحِبُّونَ أَنْ تَشِيعَ الْفَاحِشَةُ فِي الَّذِينَ آمَنُوا لَهُمْ عَذَابٌ أَلِيمٌ فِي الدُّنْيَا وَالْآخِرَةِ وَاللَّهُ يَعْلَمُ وَأَنْتُمْ لَا تَعْلَمُونَ﴾[2]، وقد أثبتت بعض الدراسات في المجتمع المصري أن (68.8%) من مجموعة المبحوثين يرون أن هناك علاقة بين الانحراف والجرائم المرتبكة وبين مشاهدة أشرطة الفيديو الجنسية، كما أثبتت إحدى الدراسات المتخصصة بتفسير ارتكاب الجريمة الجنسية في المجتمع السعودي والتي أجريت في الإصلاحيات المركزية بالدولة أن (53.7%) من مرتكبي الجرائم الجنسية كان لهم اهتمامات بالصور الجنسية وأن فئة كبيرة منهم كانوا يميلون إلى مشاهدة الأفلام الجنسية الخليعة وقت فراغهم، كما تبين من الدراسة قوة تأثير مثل هذه الصور في ارتكاب جرائم الاعتداء الجنسي من قبل مجرمي اغتصاب الإناث وهاتكي أعراض الذكور بقوة[3].

2 - المواقع المتخصصة في القذف وتشويه سمعة الأشخاص:

تعمل هذه المواقع على إبراز سلبيات الشخص المستهدف ونشر أسراره، والتي قد يتم الحصول عليها بطريقة غير مشروعة بعد الدخول على جهازه، أو بتلفيق الأخبار عنه. وهناك حادثة مشهورة جرى تداولها بين مستخدمي

(1) سورة الاسراء/الآية 32.

(2) سورة النور/الآية 19.

(3) عبد المطلب، ممدوح عبد الحميد، جرائم استخدام شبكة المعلومات العالمية (الجريمة عبر الانترنت)، المرجع السابق.

الانترنت في بداية دخول الخدمة للمنطقة حيث قام شخص في دولة خليجية بإنشاء موقع ونشر صور إحدى الفتيات وهي عارية وفي أوضاع مخلة مع صديقها، وقد حصل على تلك الصور بعد التسلل إلى حاسبها الشخصي وحاول ابتزازها جنسياً ورفضت فهددها بنشر تلك الصور على الانترنت وفعلاً قام بتنفيذ تهديده بإنشاء الموقع ومن ثم وزع الرابط لذلك الموقع على العديد من المنتديات والقوائم البريدية وأدى ذلك إلى انتحار الفتاة حيث فضحها بين ذويها ومعارفها[1]. كما وقعت حادثة تشهير أخرى من قِبل مَن اسموا نفسهم «الأمجاد هكرز»؛ حيث أصدروا بيان نشر على الانترنت بواسطة البريد الإلكتروني ووصل العديد من مشتركي الانترنت أوضحوا فيه قيام شخص يكنى بحجازي نادي الفكر على التطاول في إحدى المنتديات بالقدح والسب السافر على شيخ الإسلام ابن تيمية والشيخ محمد بن عبدالوهاب وغيرهم من رموز الدعوة السلفية، وقد استطاع (الأمجاد هكرز) اختراق البريد الإلكتروني الشخصي للمذكور ومن ثم تم نشر صوره وكشف أسراره في موقعهم على الانترنت؛ حيث خصصوا صفحة خاصة للتشهير به وحوادث التشهير والقذف في شبكة الانترنت كثيرة فقد وجد ضعفاء النفوس في شبكة الانترنت، وفي ظل غياب الضوابط النظامية والجهات المسئولة عن متابعة السلبيات التي تحدث أثناء استخدام الانترنت، متنفساً لاحقاً لهم ومرتعاً لشهواتهم المريضة دون رادع أو خوف من المحاسبة وقد قيل قديماً «من أمن العقوبة أساء الأدب». والقذف مُجَّرم شرعاً، ونظراً لشناعة الجرم ومدى تأثيره السلبي على المجني عليه والمجتمع كونه يساعد على إشاعة الفاحشة بين الناس بكثرة الترامي به، فقد جعل عقوبته من الحدود والتي لا يملك أحد حق التنازل عنه، ولا يجوز العفو عنها بعد طلب المخاصمة أمام القضاء، كما جعلها عقوبة ذات شقين الأول عقوبة بدنية بجلده ثمانين جلدة لقوله تعالى: ﴿وَالَّذِينَ يَرْمُونَ الْمُحْصَنَاتِ ثُمَّ لَمْ يَأْتُوا بِأَرْبَعَةِ شُهَدَاءَ

---

(1) المناعسة، أسامة أحمد، والزعبي جلال محمد، الهواوشة، وصايل، جرائم الحاسب الآلي والانترنت، دراسة تحليلية مقارنة، ط1، دار وائل، عمان، 2001م.

﴿فَاجْلِدُوهُمْ ثَمَانِينَ جَلْدَةً﴾[1]، والشق الثاني عقوبة معنوية بعدم قبول شهادة الجاني بعد ثبوت جلده لقوله تعالى في ذات الآية وذات السورة: ﴿وَلَا تَقْبَلُوا لَهُمْ شَهَادَةً أَبَدًا وَأُولَٰئِكَ هُمُ الْفَاسِقُونَ﴾[2] وشدد رسول الله ﷺ في جريمة القذف حيث اعتبرها من الموبقات فقال عليه الصلاة والسلام في الحديث المتفق عليه: «اجتنبوا السبع الموبقات، قالوا يا رسول الله، وما هن؟ قال الشرك بالله، والسحر، وقتل النفس التي حرم الله إلا بالحق، وأكل الربا، واكل مال اليتيم، والتولي يوم الزحف، وقذف المحصنات المؤمنات الغافلات». ولا تعاقب الشريعة على القذف إلا إذا كانَ كذباً واختلاقاً فإن كان حقيقة واقعية فلا جريمة والعقوبة[3]

3 - استخدام البروكسي للدخول إلى المواقع المحجوبة: البروكسي هو برنامج وسيط يقوم بحصر ارتباط جميع مستخدمي الانترنت في جهة واحدة ضمن جهاز موحّد، والمعنى المتعارف عليه لدى مستخدمي الانترنت للبروكسي هو ما يستخدم لتجاوز المواقع المحجوبة وهو ما نقصده في هذه الدراسة؛ حيث يستخدم البروكسي من قِبل مستخدمي الانترنت في المجتمع السعودي لتجاوز المواقع المحجوبة من قِبل مدينة الملك عبد العزيز للعلوم والتقنية والتي عادة ما تكون هذه المواقع المحجوبة أما مواقع جنسية أو سياسية معادية للدولة، وقد يتم حجب بعض المواقع التي لا يفترض حجبها كبعض المواقع العلمية والتي تنشر إحصائيات عن الجرائم أو حتى بعض المواقع العادية ويعود ذلك للآلية التي يتم بها عملية ترشيح المواقع وربما لخطأ بشري في حجب موقع غير مطلوب حجبه، ولذلك فقد تجد من يستخدم البروكسي للدخول إلى موقع علمي أو موقع عادي حجب خطأً، وهذا في حكم النادر والشاذ لا حكم له، في حين أن الغالبية العظمى تستخدم

---

(1) سورة النور/الآية 4.

(2) سورة النور/الآية 4.

(3) القاسم، محمد بن عبد الله، والزهراني، رشيد، والسند، عبد الرحمن بن عبد الله، العمري، عاطف، تجارب الدول في مجال أحكام في المعلوماتية، المرجع السابق.

البروكسي للدخول إلى المواقع الجنسية أو المواقع السياسية ولكن بدرجة أقل. ومن هنا فاستعمال البروكسي للدخول إلى المواقع المحجوبة يُعتبر أمراً مخالفاً للنظام الذي أقر حجب تلك المواقع حتى لو افترضنا جدلاً أن هناك نسبة بسيطة جداً قد تستخدم البروكسي للدخول إلى المواقع التي قد تكون حجبت بطريق الخطأ، إلا أن هذه النسبة سواء من الأفراد أو من المواقع التي تحجب بالخطأ تكاد لا تذكر وهي في حكم الشاذ، أضف إلى ذلك أنه يفترض في المواطن والمقيم احترام النظام والتقيد به دون أن يعمل بوسيلة أو بأخرى تجاوز هذا النظام لأي مبرر حتى وإن شاب النظام خلل أثناء تنفيذه، ففتح مثل هذه الثغرة والسماح للأفراد بتجاوز التعليمات التي أقرها النظام لمبرر قد يكون واهي أو لخطأ قد يكون واكب تنفيذ أمر فيه من الخطورة الشيء العظيم؛ حيث سيجرأ الأفراد على تجاوز النظام لأي مبرر وتعم الفوضى وتسود الجريمة.

المبحث العاشر

المخاطر التي تهدد خصوصية المعلومات في العصر الرقمي

تمكن تقنية المعلومات الجديدة خزن واسترجاع وتحليل كميات هائلة من البيانات الشخصية التي يتم تجميعها من قبل المؤسسات والدوائر والوكالات الحكومية ومن قبل الشركات الخاصة، ويعود الفضل في هذا إلى مقدرة الحاسبات الرخيصة، وأكثر من هذا فإنه يمكن مقارنة المعلومات المخزونة في ملف مؤتمن بمعلومات في قاعدة بيانات أخرى، ويمكن نقلها عبر البلد في ثوان وبتكاليف منخفضة نسبياً، إن هذا بوضوح يكشف إلى أي مدى يمكن أن يكون تهديد الخصوصية[1].

وتتزايد مخاطر التقنيات الحديثة على حماية الخصوصية، كتقنيات رقابة (كاميرات الفيديو) وبطاقات الهوية الإلكترونية، وقواعد البيانات الشخصية، ووسائل اعتراض ورقابة البريد والاتصالات، ورقابة بيئة العمل وغيرها[2].

إن استخدام الحاسبات في ميدان جمع ومعالجة البيانات الشخصية المتصلة بالحياة الخاصة للأفراد خلف آثاراً ايجابية، لا يستطيع أحد إنكارها خاصة في مجال تنظيم الدولة لشئون الأفراد الاقتصادية والاجتماعية والعلمية وغيرها وهذا ما أوجد في الحقيقة ما يُعرف ببنوك المعلومات (Bank Data). وقد تكون مهيأة للاستخدام على المستوى الوطني العام كمراكز وبنوك المعلومات الوطنية أو المستخدمة على نحو خاص، كمراكز وبنوك معلومات

(1) عمر ممدوح خليل، حماية الحياة الخاصة والقانون الجنائي، دار النهضة العربية، القاهرة 1983م.

(2) منصور محمد حسن، المسئولية الإلكترونية، دار الجامعة للنشر، الاسكندرية، 2003م.

الشركات المالية والبنوك وقد تكون كذلك مهيأة للاستخدام الإقليمي أو الدولي[1].

وإذا كانت الجهود الدولية والاتجاه نحو الحماية التشريعية للحياة الخاصة عموماً، وحمايتها من مخاطر استخدام الحاسبات وبنوك المعلومات على نحو خاص، تمثل المسلك الصائب في مواجهة الأثر السلبي للتقنية على الحياة الخاصة فإن هذا المسلك قد رافقه اتجاه متشائم لاستخدام التقنية في معالجة البيانات الشخصية. فالتوسع الهائل لاستخدام الحاسبات قد أثار المخاوف من إمكانات انتهاك الحياة الخاصة، وممكن إثارة هذه المخاوف، أن المعلومات المتعلقة بجميع جوانب حياة الفرد الشخصية كالوضع الصحي والأنشطة الاجتماعية والمالية والسلوك والآراء السياسية وغيرها، يمكن جمعها وخزنها لفترة غير محددة، كما يمكن الرجوع إليها جميعاً بمنتهى السرعة والسهولة. ومع الزيادة في تدفق المعلومات التي تحدثها الحاسبات، تضعف قدرة الفرد على التحكم في تدفق المعلومات عنه. أن هذه النظرة كما يظهر لنا، نظرة متشائمة من شيوع استخدام الحاسبات أثرها على تهديد الخصوصية، وهي وإن كانت نظرة تبدو مبالغاً فيها، إلا أنها تعكس حجم التخوف من الاستخدام غير المشروع للتقنية، وتحديداً الحاسبات، في كل ما من شأنه تهديد الحق في الحياة الخاصة [2]، ويمكننا فيما يلي إجمال المعالم الرئيسية لمخاطر الحاسبات وبنوك المعلومات على الحق في الحياة الخاصة بما يأتي:

1 – أن الكثير من المؤسسات الكبرى والشركات الحكومية الخاصة تجمع عن الأفراد بيانات عديدة ومفصلة تتعلق بالوضع المادي ،أو الصحي، أو التعليمي، أو العائلي، أو العادات الاجتماعية، أو العمل.. الخ، وتستخدم الحاسبات وشبكات الاتصال في خزنها

(1) قايد، أسامة عبد الله، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، المرجع السابق.

(2) عمر، ممدوح خليل، حماية الحياة الخاصة والقانون الجنائي، المرجع السابق.

،ومعالجتها، وتحليلها، والربط بينها، واسترجاعها، ومقارنتها ونقلها، وهو ما يجعل فرص الوصول إلى هذه البيانات على نحو غير مأذون به أو بطريق التحايل أكثر من ذي قبل [1].

2 - شيوع النقل الرقمي للبيانات خلق مشكلة أمنية وطنية، إذ سهل استراق السمع والتجسس الإلكتروني. ففي مجال نقل البيانات تتبدى المخاطر المهددة للخصوصية في عدم قدرة شبكات الاتصال على توفير الأمان المطلق أو الكامل لسرية ما ينقل عبرها من بيانات، وإمكانية استخدام الشبكات في الحصول بصورة غير مشروعة، عن بعد على المعلومات[2].

إن بدء مشكلات الكمبيوتر في الستينات ترافق مع الحديث - في العديد من الدول الغربية - عن مخاطر جمع وتخزين وتبادل ونقل البيانات الشخصية ومخاطر تكنولوجيا المعلومات في ميدان المساس بالخصوصية والحريات العامة، وانتشر الحديث عن الخطر الكبير الذي يُهدد الحرية الشخصية بسبب المقدرة المتقدمة لنظم المعالجة الإلكترونية على الكشف والوصول إلى المعلومات المتعلّقة بالأفراد واستغلالها في غير الأغراض التي تجمع من أجلها. وخلال الثمانينات تغير الواقع التكنولوجي فيما يتعلّق بالجهات التي تملك وتسيطر على نظم الكمبيوتر وكان ذلك بسبب إطلاق الحاسبات الشخصية وانتشارها، وأصبح من الواضح أن حماية الخصوصية يتعين أن تمتد إلى الكمبيوترات الخاصة وأن يتم إحداث توازن ما بين الحق في الخصوصية أو الحق في الحياة الخاصة وبين الحق في الوصول إلى المعلومات، هذا التغير في الواقع التكنولوجي عكس نفسه على حقل الحماية القانونية في الخصوصية بأبعادها التنظيمية والمدنية والجزائية وبدأت تكثر الأحاديث بشأن دعاوى الاستخدام غير المشروع للمعلومات وللوثائق

(1) هلال، محمد رضوان، المحكمة الرقمية، المرجع السابق.

(2) عمر، ممدوح خليل، حماية الحياة الخاصة والقانون الجنائي، المرجع السابق.

الشخصية، وظهرت أحداث شهيرة في حقل الاعتداء على البيانات الخاصة من بينها على سبيل المثال الحادثة التي حصلت في جنوب أفريقيا حيث أمكن للمعتدين الوصول إلى الأشرطة التي خزّنت عليها المعلومات الخاصة بمصابي أمراض الإيدز وفحوصاتهم، وقد تم تسريب هذه المعلومات الخاصة والسرية إلى جهات عديدة. ومن الحوادث الشهيرة الأخرى حادثة حصلت عام 1989 م عندما تمكن أحد كبار موظفي أحد البنوك السويسرية بمساعدة سلطات الضرائب الفرنسية بأن سرَّب إليها شريطاً يحتوي على أرصدة عدد من الزبائن، وقد تكرر مثل هذا الحادث في ألمانيا أيضاً [1].

إن هذه المخاطر أثارت وتثير مسألة الأهمية الاستثنائية للحماية القانونية - إلى جانب الحماية التقنية - للبيانات الشخصية، ومن العوامل الرئيسية في الدفع نحو وجوب توفير حماية تشريعية وسن قوانين في هذا الحقل، أنه وقبل اختراع الكمبيوتر فإن حماية هؤلاء الأشخاص كانت تتم بواسطة النصوص الجنائية التي تحمي الأسرار التقليدية (كحماية الملفات الطبية أو الأسرار المهنية بين المحامي والموكل)، وعلى الرغم من ذلك فإن هذه النصوص التقليدية لحماية شرف الإنسان وحياته الخاصة لا تغطي إلا جانباً من الحقوق الشخصية وبعيدة عن حمايته من مخاطر جمع وتخزين والوصول إلى ومقارنة واختيار وسيلة نقل المعلومات في بيئة الوسائل التقنية الجديدة هذه المخاطر الجديدة التي تستهدف الخصوصية دفعت العديد من الدول لوضع تشريعات ابتداء من السبعينات من القرن العشرين تتضمن قواعد إدارية ومدنية وجنائية من أجل حماية الخصوصية وتوصف بأنها تشريعات السرية وليست فقط مجرد تشريعات تحمي من افعال مادية تُطال الشرف والحياة الخاصة [2]. كما أن هذه المخاطر، وما يتفرَّع عنها من مخاطر

---

(1) Taylor (R.): Computer crime, "in criminal investigation edited" by Charles Swanson, n. chamelin and L. Territto, Hill, inc. 5 edition 1992.

(2) الفيومي، محمد، «مقدمة في علم الحاسابات الإليكترونية والبرمجة بلغة بيسك»، المرجع السابق.

أخرى كتلك الناتجة عن معالجة البيانات في شبكات الحاسبات المربوطة ببعضها البعض والتي تُتيح تبادل المعلومات بين المراكز المتباعدة والمختلفة من حيث أغراض تخزين البيانات بها نقول أن هذه المخاطر كانت محل اهتمام دولي وإقليمي ووطني أفرز قواعد ومبادئ تتفق وحجم هذه المخاطر، كوجوب مراعاة الدقة في جمع البيانات وكفالة صحتها وسلامتها، واتخاذ تدابير أمنية لمعالجتها وخزنها ونقلها، وإقرار مبدأ حق المشاركة الفردية في تعديل وتصحيح وطلب إلغاء البيانات، ووجوب تحديد الغرض من حجمها ومدة استخدامها، وإقرار مبدأ مسئولية القائمين على وظائف بنوك المعلومات لأي تجاوز أو مخالفة للمبادئ الموضوعية والشكلية في جمع ومعالجة وتخزين ونقل البيانات الشخصية[1].

وكما نعلم أن الانترنت لا يعترف بالحدود، فالمكان والزمان عنصران غالباً ما لا يكون لهما أي أثر في أنشطة تبادل المعلومات والعلاقات الناشئة في بيئة الانترنت، وللانترنت سمات وخصائص ذات اثر على البناء القانوني والعلاقات القانونية، فهي واسطة اتصال تنقل فيها المعلومات على شكل حزم، توجه إلى عنوان افتراضي لا صلة له بالمكان بوجه عام، وليس ثمة طريق اتصال محدَّد من نقطة إلى نقطة، إنما انتقال عشوائي يتخير بذكاء أفضل الطرق واقصرها للوصول إلى مقصده النهائي، هذه الحزمة تحمل معلومة أو رسالة بريد إليكتروني، أو برنامجاً، أو طلباً، أو غير ذلك، وليس ثمة سيطرة مركزية لأحد على الانترنت، أنها بيئة مملوكة لكافة الأفراد والمؤسسات وليست مملوكة لأحد، وليس ثمة إطار تقني، أو قانوني، أو تنظيمي يسيطر مركزياً على الانترنت بل إن إداراتها والتحكّم بها إنما تحكمه طبائعها الذاتية وواقع (حركة السير) لملايين الاتصالات التي تتم في نفس الوقت[2].

---

(1) قايد، أسامة عبد الله، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، المرجع السابق.

(2) عرب، يونس، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، منشورات إتحاد المصارف العربية، الطبعة الأولى،

أما أثر التقنية على القانون وفي مدى انسجام بعض الدعوات الدولية لحد أدنى من التنظيم القانوني لتقنية المعلومات مع واقع النظام القانوني العربي والتقنية العالية أحدثت منذ نهاية الستينات آثاراً واسعة على العلاقات القانونية والتصرفات القانونية أوجدت وخلقت فروعاً وموضوعات قانونية استلزمت موجات متلاحقة من التشريعات، وذلك في ثمانية حقول، أمن المعلومات - جرائم الكمبيوتر والانترنت - ومسائل الخصوصية وحماية الحياة الخاصة، ومسائل الملكية الفكرية للمصنفات الرقمية كالبرمجيات والدوائر المتكاملة وقواعد البيانات، وأسماء نطاقات وعناوين الانترنت وحماية محتوى مواقع المعلوماتية، وكذلك في حقول المعايير والمقاييس التقنية، وفي حقل قواعد الإثبات والإجراءات الجنائية وما تبعها من مسائل الاختصاص والقانون الواجب التطبيق، وفي حقل وسائل الدفع الإليكتروني والخدمات المصرفية الإليكترونية، وتثير الآن أوسع تحدياتها في حقل التجارة الالكترونية والحكومة الإليكترونية التي مثّلت الإطار الجامع لحركة التشريع المتصل بتقنية المعلومات، وقد كان من أهم انتقادات الفقهاء بشان التدابير التشريعية لمسائل تقنية المعلومات أن التدخل قد تم في كل موضوع على حده واستقلال عن غيره، ولهذا دعا هؤلاء إلى فرع قانوني جديد هو قانون الكمبيوتر [1]، لكن ومن حيث لم يتوقع أحد، جاءت التجارة الإليكترونية لتخلق الحاجة إلى إيجاد تنظيم شمولي للمسائل القانونية المتصلة بتقنية المعلومات في كافة فروعها، فالتجارة الإليكترونية أظهرت الأهمية للتدخل التشريعي لتنظيم مسائل الخصوصية وأمن المعلومات والحجية القانونية للمستخرجات ذات الطبيعة الإليكترونية ومسائل الملكية الفكرية وأسماء النطاقات وعلاقتها بالعلامات التجارية ومسائل التوثق والتعريف الشخصي والتواقيع الرقمية والتشفير ومعايير الخدمات التقنية ومواصفاتها والتنظيم القانوني لسوق

2000م.

(1) حجازي، سهير، التهديدات الإجرامية للتجارة الإليكترونية، مركز البحوث والدراسات، شرطة دبي بدولة الإمارات العربية المتحدة، 2005م.

الخدمات التقنية ومسائل الضرائب إضافة إلى مسائل الحق في الوصل للمعلومات التي إثارتها بشكل رئيس فكرة الحكومة الإليكترونية وبقية فروع قانون الكمبيوتر ذات العلاقة [1].

وانطلاقاً من هذه الحقيقة علينا أن ندرك كدول عربية الاختلاف فيما بين الواقع الدولي وواقع أنظمتنا القانونية في تعاملهما مع مسائل تقنية المعلومات، وصحيح أن هناك شبه إجماع عالمي على وجوب أن يكون التدخل التشريعي في التجارة الإليكترونية بحدوده الدنيا وهذا ما عبرت عنه الرئاسة الأمريكية في عام 1997م عند إطلاق إطار التجارة الإليكترونية وهو ما تبناه خبراء الاتحاد الأوروبي في مؤتمراتهم وهو ما تبناه المؤتمر العالمي لمنظمة التعاون الاقتصادي والتنمية عام 1998م، لكن لهذه الجهات أن تتبنى هذا الموقف لأن نظمها القانونية عرفت عشرات التشريعات في حقل تقنية المعلومات قبل التجارة الإليكترونية، ولأن نظمها منذ مطلع السبعينات عرفت حزمة تشريعات لا تزال آخذة في النماء والتطور في حقل جرائم الكمبيوتر وأمن المعلومات وحجية مستخرجات الحاسب والمواصفات والمعايير التقنية والملكية الفكرية والخصوصية وقواعد نقل وتبادل البيانات ووسائل الدفع الإليكتروني وحماية المستهلك وغيرها، لكن مجتمعاتنا لم تعرف مثل هذه التشريعات ولم تتقاطع مع موجات التشريع العالمية في هذا الميدان، أضف إلى ذلك أن ثمة عشرات الاتفاقيات الدولية والثنائية في حقل حماية البيانات ونقلها وفي حقل الحماية الجنائية من الأنشطة الجريمة في عالم المعلومات[2].

نحن لسنا طرفاً فيها وليس بين دولنا العربية حد أدنى من مثل هذا التعاون. لهذا لا يصلح معنا كدول عربية تبني وجهة النظر التي تطالب بحد أدنى من التدخل التشريعي دون تقييم هذه الدعوى، فهي صحيحة للغير

---

(1) علي، عبد الصبور عبد القوي، التجارة الإليكترونية والقانون، دار العلوم للنشر والتوزيع، القاهرة 2007م.

(2) منصور، محمد حسن، المسئولية الإليكترونية، المرجع السابق.

وليست صحيحة لنا ببساطة لأنهم أنجزوا وينجزون مئات التشريعات والأطر القانونية في هذا الحقل ونحن بعد لم نقف على أي من موجات التشريع هذه، ولهذا فإن الدول العربية مدعوة لوقفة أكثر شمولية ودقة في إرساء تنظيم تشريعي شمولي لإفرازات عصر المعلومات ومن هنا تجدونني أومن بأن استراتيجيتنا العربية هي بناء الـ E - Law، أي بناء النظام القانوني المتوائم مع العصر الإليكتروني، وهي برأيي وسيلة حقيقة لإنتاج معارفنا القانونية الخاصة والكف عن سياسات استهلاك معارف الآخرين سيما وإن شرائعنا السماوية وحركة تعاملنا مع التاريخ تدعونا لأن نكون نحن لا أن نكون مستهلكين لخيارات الآخرين [1].

---

(1) مصلح، يحيى، التجارة على الانترنت. سايمون كولن، نقله إلى العربية، بيت الأفكار الدولية بأمريكا 1999م.

الفصل الثاني

اختصاصات المحكمة الرقمية والجريمة المعلوماتية

مقدمة:

مما لا شك فيه أن المحكمة الرقمية هي محكمة متخصصة في نظر الدعاوى والقضايا التي تُرتكب عبر الانترنت سواء كانت هذه الدعاوى جنائية وكذلك نظر الدعاوى المدنية والعقود الإليكترونية وكافة منازعات التجارة الإليكترونية بواسطة قضاة برعوا في دراسة وتطبيق قوانين وأنظمة تقنية المعلومات وقد عرف النظام السعودي الحاسب الآلي في المادة الأولى من نظام التعاملات الإليكترونية بأنه: «أي جهاز إليكتروني ثابت أو منقول، سلكي أو لاسلكي، يحتوي على نظام معالجة البيانات، أو تخزينها، أو إرسالها، أو استقبالها، أو تصفحها يؤدي وظائف محددة بحسب البرامج والأوامر المعطاة له» (مادة أولى فقرة 7 من نظام التعاملات الإليكترونية والمادة الأولى فقرة 6 من نظام مكافحة الجرائم المعلوماتية وعرفت المادة نفسها كلمة «إليكتروني» بأنها: «تقنية استعمال وسائل كهربائية، أو كهرومغناطيسية أو بصرية أو أي شكل آخر من وسائل التقنية المشابهة» (مادة أولى - 9). كما عني نظام التعاملات الإليكترونية في المملكة ببيان المقصود بالتعاملات الإليكترونية بتعريفها وذلك بقوله: «التعاملات الإليكترونية: أي تبادل أو تراسل أو تعاقد، أو أي إجراء آخر يبرم أو ينفذ - بشكل كلي أو جزئي - بوسيلة إليكترونية».

(مادة أولى - 10). كما أوضح مفهوم البيانات الإليكترونية بقوله «البيانات الإليكترونية: بيانات ذات خصائص إليكترونية في شكل نصوص، أو رموز، أو صور، أو رسوم، أو أصوات، أو غير ذلك من الصيغ الإليكترونية، مجتمعة أو متفرقة». (مادة أولى - 11). وعرّف النظام أو منظومة البيانات الإليكترونية بقوله «منظومة بيانات إليكترونية: جهاز أو برنامج إليكتروني أو أكثر يستخدم لإنشاء البيانات الإليكترونية، أو استخراجها، أو إرسالها، أو بثها، أو تسلمها ،أو تخزينها، أو عرضها، أو معالجتها». وقد بدأ إدراك أهمية الموضوع يتزايد وفي بعض التشريعات العربية مثل التشريع التونسي الذي كان له فضل السبق في - بين تشريعات الدول العربية - سن قانون خاص بالتجارة الإليكترونية وهو القانون رقم 83 لسنة 2000م الصادر في أغسطس سنة 2000 م في شأن المبادلات والتجارة الإليكترونية. كما أصدرت إمارة دبي في دولة الإمارات العربية المتحدة قانوناً خاصاً بالتعاملات الإليكترونية وهو القانون رقم (2) لسنة 2002 م بشأن المعاملات والتجارة الإليكترونية، كما صدر القانون الاتحادي في دولة الإمارات العربية المتحدة رقم (2) لسنة 2006م، وقبل ذلك عرف قانون الجزاء العماني رقم 74/7 منذ سنة 2001 م جرائم الكمبيوتر والانترنت. وفي مصر صدر القانون رقم 15 في شأن تنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات بتاريخ 22 أبريل سنة 2004 م. وقد أحسن المنظِّم السعودي صنعاً عندما أصدر نظامي المعاملات الإليكترونية ومكافحة جرائم المعلوماتية الصادرين في 1428/3/7 هـ الموافق 2007/3/26م. لذلك كان لزاماً علينا أن نتعرَّض في هذا الفصل إلى معرفة الاختصاص في النظام السعودي بوجه عام وأنواع الاختصاص واختصاصات المحكمة الرقمية وذلك فيما يلي:

المبحث الأوّل

مفهوم الاختصاص بوجه عام

الاختصاص في اللغة:

مأخوذ من مادة خَصَّ، تقول: اختصَّ فلان بكذا، إذا انفرد به دون غيره، واختصَّه بالشيء، إذا خصه به وفضله واختاره واصطفاه، والتخصيص ضد التعميم[1].

الاختصاص في اصطلاح النظام القضائي:

«السلطة التي خولها القانون لمحكمة ما في الفصل في نزاع ما»[2].

يتَّضح العلاقة لنا مما تقدم الوثيقة بين المعنى اللغوي والمعنى الاصطلاحي. فالاختصاص كما سلف يأتي بمعنى الانفراد والاصطفاء ونقيض التعميم. وهذا المعنى واضح وجلي في المعنى الاصطلاحي؛ حيث فيه انفراد هذه الجهة القضائية عن غيرها بهذه القضية لصفة وجدت فيها مما جعلها تختص بها دون سواها، لذا اختيرت لهذه المهمة والنوع، إذ الخصوصية [3] لا تكون إلا لصفة توجد في شيء ولا توجد في غيره.

---

(1) القاموس المحيط، باب الصاد، فصل الخاء، ص570، ولسان العرب 109/4، والمعجم الوسيط1/238.

(2) قانون المرافعات المدنية والتجارية، ص245، والوسيط في شرح قانون المرافعات المدنية والتجارية، ص355.

(3) كما جاء في معجم لغة الفقهاء، ص174.

المبحث الثاني

الاختصاص القضائي في النظام السعودي

أُنْشِأت المحاكم في المملكة العربية السعودية التي تحَكِّم شرع الله على اختلاف درجاتها واختصاصاتها، كما أُصدرت الأنظمة واللوائح - والتي تطورت مؤخراً - لترتب شئون هذه المحاكم، وتبين حدودها وصلاحياتها [1].

فمن أولى الخطوات الأمر بتشكيل المحاكم وتحديد اختصاصاتها: صدور المرسوم الملكي في عام 1346هـ يقضي بإنشاء المحاكم على ثلاث درجات، وهي:

«1 - محاكم الأمور المستعجلة (محاكم جزئية).

2 - محاكم كبرى، ومحاكم ملحقات، وهما عبارة عن محاكم عامة.

3 - هيئة المراقبة القضائية (محكمة التمييز).

وقد تضمن المرسوم النص على اختصاصاتها.

فالجهود مبذولة في سبيل رفع مستوى الأداء في الجهاز القضائي بسن الأنظمة، وبناء المحاكم، وتعيين القضاة المتخصصين في القضايا المختلفة.

المطلب الأوّل

الاختصاص الدولي

الاختصاص القضائي الدولي هو بيان القواعد التي تحدد ولاية محاكم الدولة في المنازعات التي تتضمن عنصراً أجنبياً إزاء غيرها من محاكم الدولة

(1) المصدر السابق، ص279؛ والنظم الإسلامية، ص33-34.

الأخرى، وذلك بالمقابلة لقواعد الاختصاص الداخلي والتي تُحدد اختصاص كل محكمة من محاكم الدولة إزاء غيرها من محاكم الدولة نفسها [1].

ونجد أن المنظِّم عند تشريعه للقواعد المتعلّقة بالاختصاص الدولي جعل معايير واعتبارات ينعقد على أساسها الاختصاص للمحاكم وفقاً لنظام المرافعات ومن ذلك:

1 - معيار الجنسية.

2 - معيار الإقامة.

3 - معيار طبيعة الدعوى.

4 - معيار الرضا بالاختصاص.

المطلب الثاني

الاختصاص الولائي في النظام السعودي

ويُقصد بهذا الاختصاص: تحديد نصيب كل جهة قضائية من جهات التقاضي من ولاية القضاء. ويُسمَّى: اختصاص الجهة»[2]. والاختصاص الولائي يُعد نوعاً من أنواع الاختصاص النوعي بمعناه العام.

ويُعتبر الاختصاص الولائي أو الوظيفي اختصاصاً مطلقاً؛ لتعلُّقه بالنظام العام للدولة؛ لأنه مقرر لمصلحة عامة [3].

---

(1) تنازع الاختصاص القضائي، ص 5.

(2) انظر: قانون المرافعات المدنية والتجارية، ص249، والوسيط في شرح قانون المرافعات، ص355؛ والقواعد الإجرائية في المرافعات الشرعية، ص98.

(3) انظر: قانون المرافعات المدنية والتجارية، ص254.

ويتمثّل الاختصاص الولائي في المملكة في الآتي:

أولاً: ولاية القضاء الشرعي (العادي).

ثانياً: ولاية قضاء المظالم (القضاء الإداري).

فالقضاء العادي هو: جهة القضاء ذات الولاية العامة بنظر المنازعات والجرائم فلا يخرج من اختصاصه إلا ما أدخله المنظّم في الاختصاص الإداري أو ما قد يخرجه المنظّم بنص خاص، فالقضاء الإداري بمقابلة القضاء العادي هو جهة قضاء تقتصر ولايته على نظر المسائل الإدارية فهو جهة قضاء محدودة الولاية [1].

أولاً: ولاية القضاء الشرعي (العادي):

جاء في المادة (26) من نظام القضاء ما نصه: «تختص المحاكم بالفصل في كافة المنازعات، والجرائم إلا بما يُستثنى بنظام، وتبين قواعد اختصاص المحاكم في نظامي المرافعات والإجراءات الجزائية، ويجوز إنشاء محاكم متخصصة بأمر ملكي بناء على اقتراح مجلس القضاء الأعلى [2].

ثانياً: ولاية قضاء المظالم (القضاء الإداري):

جاء في المادة الأولى من نظام ديوان المظالم ما نصه: - ديوان المظالم هيئة قضاء إداري مستقلة ترتبط مباشرة بجلالة الملك.

وفصلت المادة الثامنة من نظام الديوان اختصاصاته وهي:

أ - الدعاوى المتعلّقة بالحقوق المقررة في نظم الخدمة المدنية والتقاعد لموظفي ومستخدمي الحكومة والأجهزة ذوات الشخصية المعنوية العامة المستقلة أو ورثتهم والمستحقين عنهم.

ب - الدعاوى المقدّمة من ذوي الشأن بالطعن في القرارات الإدارية

---

(1) الوسيط في شرح قانون المرافعات، ص 359

(2) انظر نظام القضاء الصادر بالمرسوم الملكي رقم 648/م تاريخ 1395/7/14هـ.

متى كان مرجع الطعن عدم الاختصاص، أو وجود عيب في الشكل، أو مخالفة النظم واللوائح، أو الخطأ في تطبيقها، أو تأويلها، أو إساءة استعمال السلطة، ويُعتبر في حكم القرار الإداري رفض السلطة الإدارية أو امتناعها عن اتخاذ قرار كان من الواجب عليها اتخاذه طبقاً للأنظمة واللوائح.

ج - دعاوى التعويض الموجهة من ذوي الشأن إلى الحكومة والأشخاص ذوي الشخصية العامة المستقلة بسبب أعمالها.

د - الدعاوى المقدَّمة من ذوي الشأن في المنازعات المتعلِّقة بالعقود التي تكون الحكومة، أو أحد الأشخاص المعنوية العامة طرفاً فيها.

هـ - الدعاوى التأديبية التي تُرفع من هيئة الرقابة والتحقيق.

و - الدعاوى الجزائية الموجهة ضد المتهمين بارتكاب جرائم التزوير المنصوص عليها نظاماً، والجرائم المنصوص عليها في نظام مكافحة الرشوة، والجرائم المنصوص عليها في المرسوم الملكي رقم 43 وتاريخ 77/11/29هـ، والجرائم المنصوص عليها في نظام مباشرة الأموال العامة الصادر بالمرسوم الملكي رقم 77 وتاريخ 95/10/23هـ، وكذلك الدعاوى الجزائية ضد المتهمين بارتكاب الجرائم والمخالفات المنصوص عليها في الأنظمة إذا صدر أمر من رئيس مجلس الوزراء إلى الديوان بنظرها.

ز - طلبات التنفيذ الأحكام الأجنبية.

ح - الدعاوى التي من اختصاص الديوان بموجب نصوص نظامية خاصة.

وجاء أيضاً في المادة (الحادية والثلاثون) من نظام المرافعات الشرعية ما يدل على وجوب الأخذ بقواعد الاختصاص الولائي، أو الوظيفي، وجعلها في جهتين:

الجهة الأولى: القضاء العادي المتمثّل بالمحاكم العامة والجزئية.

والجهة الثانية: القضاء الإداري المتمثّل في ديوان المظالم. ونص المادة: (من غير إخلال بما يقضي به نظام ديوان المظالم، وبما للمحاكم العامة من اختصاص في نظر الدعوى العقارية، تختص المحاكم الجزئية بالحكم في الدعاوى الآتية:

أ – دعوى منع التعرُّض للحيازة ودعوى استردادها.

ب – الدعاوى التي لا تزيد قيمتها على عشرة آلاف ريال، وتحدد اللائحة التنفيذية كيفية تقدير قيمة الدعوى.

ج – الدعوى المتعلّقة بعقد إيجار لا تزيد الأجرة فيه على ألف ريال في الشهر بشرط ألا تتضمن المطالبة بما يزيد على عشرة آلاف ريال.

د – الدعوى المتعلّقة بعقد عمل لا تزيد الأجرة، أو الراتب فيه على ألف ريال في الشهر بشرط ألا تتضمن المطالبة بما يزيد على عشرة آلاف ريال.

ويجوز عند الاقتضاء تعديل المبالغ المذكورة في الفقرات (ب، جـ، د) من هذه المادة، وذلك بقرار من مجلس القضاء الأعلى بهيئته العامة بناءً على اقتراح من وزير العدل).

المطلب الثالث

الاختصاص النوعي في النظام السعودي

ويقصد بالاختصاص النوعي في النظام:

«توزيع العمل بين المحاكم المختلفة في داخل الجهة القضائية الواحدة بحسب نوع القضية»[1].

(1) الوسيط في شرح قانون المرافعات المدنية والتجارية، ص288.

ويُعتبر تخصيص عمل القضاة، وإنشاء المحاكم المتخصصة ضرورة عصرية ملحة؛ نتيجة ازدياد المنازعات، وتنوع مشاكل العصر، وتشعبها، وتداخلها، وكذلك نتيجة تعدد الأنظمة لمسايرة متطلبات العصر، فلأجل هذه الاعتبارات وغيرها، اتجهت الأنظمة القضائية المعاصرة إلى الأخذ بنظام تخصص القضاة، نظراً لتزايد القضايا التي يتعسَّر أو يتعذَّر على القاضي إنهاؤها على الوجه المنشود؛ مما قد يدفع القاضي للتعجيل في إصدار الأحكام وحينئذٍ قد تصدر الأحكام دون رَوِيَّة، وإما أن يتروى فيستغرق ذلك وقتاً طويلاً؛ الأمر الذي يترتب عليه تأخير الفصل في المنازعات وفي الحالين قد لا يستقيم معه العمل لذلك اتجهت الأنظمة القضائية المعاصرة إلى الأخذ بنظام تخصص القضاة [1]. فتتخصص كل من المحاكم بالمسائل التي ترفع إليها طبقاً للنظام.

وقد عالج مثل ذلك نظام المرافعات الشرعية وأيضاً لوائحه التنفيذية الصادرة بالقرار الوزاري 4569 وتاريخ 1423/6/3هـ لتكون القواعد التي يسير عليها القائم بالعمل القضائي، ولأهميتها قد أفرد المنظِّم لها الباب الثاني تضمنت ثلاثة فصول واشتملت على خمسة عشر مادة.

المطلب الرابع

الاختصاص القيمي في النظام السعودي

فيقصد به: «سلطة المحكمة في الفصل في الدعوى حسب قيمتها، بغض النظر عن نوعها»[2].

وقيل هو: «مجموعة من القواعد التي تستهدف تحديد المحكمة المختصة

---

(1) المصدر السابق، ص369-370.

(2) التعليق على نصوص نظام المرافعات الشرعية 238/1.

بنظر الدعوى؛ وذلك على ضوء قيمتها»[1].

والاختصاص هو: «اختصاص كل طبقة من طبقات المحاكم داخل الولاية القضائية الواحدة بحسب قيمة الدعوى».

ولقد أخذ النظام السعودي هذا النوع من الاختصاص القضائي؛ حيث اعتدَّ بالقيمة المالية في دعوى الحقوق المالية عند المنازعة كمعيار لتوزيع الاختصاص النوعي بين المحاكم الجزئية والمحاكم العامة، حيث نص قرار معالي وزير العدل رقم (2514) بتاريخ (1417/5/13هـ) على اختصاص المحاكم الجزئية بالنظر في أروش الجنايات التي لا تزيد على ثلث الدية، وفي منازعات الحقوق المالية فيما لا تتجاوز عشرين ألف ريال سعودي.

وهـذا يعني أن كل ما زاد على تلك القيمة فإنها تكون من اختصاص المحكمة العامة. علماً أن تحديد قيمة الدعوى لم ترد في نظَام المرافعات إنما في اللائحة التنفيذية التي أحال إليها النظَام كما في (المادة الواحدة والثلاثين فقرة ب والمادة الواحدة والثلاثين فقرة د) أجازت حق تعديل قيمة الدعاوى لمجلس القضاء الأعلى بناءً على اقتراح يقدمه وزير العدل تجاه تعديل النصاب الذي يدخل في اختصاص المحكمة الجزئية.

ففي ظل نظام المرافعات ووفقاً للمادة الواحدة والثلاثين المذكورة تختص المحاكم الجزئية بالدعاوى التي لا تزيد قيمتها على عشرة آلاف ريال (والذي حُدد لاحقاً بعشرين ألف ريال بقرار مجلس القضاء الأعلى بهيئته العامة رقم 54/361 وتاريخ 1422/11/20هـ المعمم بخطاب معالي وزير العدل رقم 13/ت/1911 في 1422/12/21هـ.

وإن جعل تحديد تقدير الدعوى للائحة التنفيذية وكذا تعديل مبلغ قيمة الدعوى التي تدخل في اختصاص المحكمة الجزئية بقرار يصدر من

(1) قانون المرافعات المدنية والتجارية، ص353؛ والوسيط في شرح قانون المرافعات، ص410.

مجلس القضاء الأعلى بناءً على اقتراح من وزير العدل يعتبر محققاً للمرونة قد لا يمكن معه إذا ترك ذلك للنظام، ذلك أن إصدار اللائحة أو القرار أيسر في الصدور أو التعديل، فيجعل النظّام مواكباً بما تُقرره اللائحة لطبيعة الأوضاع الاقتصادية وحالتها.

ومما يؤكّد تحقيق النوعية في الاختصاص كما هو وارد في المادة الواحدة والثلاثين من نظّام المرافعات فقد ذكرت عدداً من الدعاوى وجعل الاختصاص بها للمحكمة الجزئية. وقد جعل الدعاوى غير الواردة في اختصاص المحكمة الجزئية منعقدة للمحاكم العامة.

ثم ورد في المادة التي تليها بعض من الدعاوى التي تدخل في اختصاص المحكمة العامة بحسب نوعيتها؛ فجعل للمحكمة العامة الاختصاص نوعاً في:

أ - الدعاوى العينية المتعلّقة بالعقار حتى ولو كانت قيمة العقار أقل أو تساوي عشرة آلاف ريال.

ب - دعاوى النفقة حتى لو كان قدر المطالب به يدخل في ضمن نصاب المحكمة الجزئية كما جاء بيانه في تكملة المادة المذكورة كما سيتبين لاحقاً عند ذكر المواد.

فالمتأمل يجد أن هناك تداخلاً فيما يتعلّق بالاختصاص النوعي مع الاختصاص القيمي كما ذكرناه آنفاً؛ وهو بذلك يدخل ضمن ما صنّفه بعض القانونيين من دخول الاختصاص القيمي ضمناً في الاختصاص النوعي الذي يقوم على معيارين:

- أحدهما نوع الدعوى.
- والآخر قيمة الدعوى[1].

---

(1) سرور، أحمد فتحي، الوسيط في الإجراءات الجنائية، دار النهضة العربية، القاهرة 1985م.

المطلب الخامس

الاختصاص المحلي في النظام السعودي

ويُقصد به: «سلطة المحكمة في نظر الدعوى التي تقع في دائرة اختصاصها المكاني أو الجغرافي بناء على معيار معين»[1]. وعرفه بعضهم بأنه: «مجموعة القواعد التي تعين المحكمة المختصة من بين عدة محاكم من نوع واحد موزعة في المدن والبلدان من المملكة للنظر في قضية معينة»[2].

والقاعدة المبنية عليه هذا الاختصاص المحلي هو رعاية مصلحة الخصوم، وخاصة المدَّعى عليه؛ لأن الأصل البراءة، فتقرر الاختصاص لمحكمة قريبة منه، أو من محل النزاع؛ لتكون العدالة في متناول المتقاضين، ولا تكون بعيدة عنهم [3].

«وبناءً على هذا فالذي استقر عليه العمل هو أن ما نصت عليه المادة (38) من نظام المرافعات الشرعية أن: «تعد المدينة أو القرية نطاقاً محلياً للمحكمة الموجود بها. وعند تعدد المحاكم فيها يحدد وزير العدل النطاق المحلي لكل منها بناء على اقتراح من مجلس القضاء الأعلى. وتتبع القرى التي ليس بها محاكم محكمة أقرب بلدة إليها. وعند التنازع على الاختصاص المحلي إيجابياً أو سلبياً تُحال الدعوى إلى محكمة التمييز للبت في موضوع التنازع»[4].

المطلب السادس

الاختصاص الزماني في النظام القضائي

لقد أخذ النظام بمبدأ تخصيص عمل القاضي بالزمان، ويتضح ذلك من خلال الأمور التالية:

(1) التعليق على نصوص نظام المرافعات الشرعية1/260.
(2) التنظيم القضائي في المملكة العربية السعودية، ص444.
(3) الاختصاص القضائي في الفقه الإسلامي، ص420.
(4) التعليق على نصوص نظام المرافعات الشرعية1/272.

نصت المادة (55) من نظام القضاء بما نصه: «وتكون مدة الندب أو الإعارة سنة واحدة، قابلة للتجديد سنة أخرى، على أنه يجوز لوزير العدل في الحالات الاستثنائية أن يندب أحد أعضاء سلك القضائي داخل السلك أو خارجه لمدة لا تتجاوز ثلاثة أشهر في العام الواحد».

فقد يكلف أحد القضاة بالعمل في منطقة أخرى لسبب من الأسباب، غير المنطقة التي يعمل فيها، وتحدد له مدة زمنية يرجع إليها؛ فهذا القاضي المنتدب صارت ولايته في المكان الجديد محددة بالزمن، بحيث لا يقضي في تلك البلدة قبلها ولا بعدها. وقد نصت نظام القضاء في المادة (55) بما نصه: «وتكون مدة الندب أو الإعارة سنة واحدة، قابلة للتجديد سنة أخرى، على أنه يجوز لوزير العدل في الحالات الاستثنائية أن يندب أحد أعضاء سلك القضائي داخل السلك أو خارجه لمدة لا تتجاوز ثلاثة أشهر في العام الواحد».

ومثله أيضاً عند بدء الإجازة الرسمية للمحاكم في أيام الحج والعيدين يكلّف بعض القضاة للعمل فيها [1].

---

(1) التصنيف الموضوعي 479/4. تعميم رقم 102/4/5ت في 1407/6/12هـ

المبحث الثالث

تنازع الاختصاص واختصاص الجرائم المعلوماتية في النظام السعودي

المطلب الأوّل

تنازع الاختصاص في النظام السعودي

التنازع على الاختصاص هو ظاهرة تنشأ حتماً عن نظام توزيع الاختصاص على محاكم الجهة القضائية الواحدة في الدولة، فقد ترى كل محكمة أن المنازعة أو المسألة المرفوعة إليها تخرج عن نطاق اختصاصها فتنفي اختصاصها بها وترفض مباشرة نظرها والفصل فيها، ويتحقّق هذا النزاع على الاختصاص في حالة ما إذا رفعت نفس الدعوى أمام محكمتين مختصتين - كما في حالات الاختصاص المشترك - فتتنازع المحكمتان الاختصاص بالدعوى، سواء بأن تدفع كل محكمة بعدم اختصاصها بها (التنازع السلبي) أو بأن تُقرِّر كل منهما اختصاصها بالدعوى (التنازع الإيجابي) فتستمر في نظرها وهو ما قد يؤدي إلى صدور حكمين متناقضين في مسألة واحدة أو دعويين مرتبطتين ينشأ تنازع في تنفيذهما [1].

وهذا التنازع على الاختصاص الذي ينشأ بين محاكم الجهة القضائية الواحدة، وقد ينشأ التنازع بين جهتين قضائيتين، مثل نظام ديوان المظالم «القضاء الإداري» جهة المحاكم «القضاء العادي» لا بين محاكم جهة واحدة، فقد يكون تنازعاً سلبياً، عندما تتخلى كلتا الجهتين عن نظر النزاع، وقد يكون تنازعاً إيجابياً عندما تقرر كل منهما اختصاصها بنظر النزاع، أو أن

(1) أصول وقواعد المرافعات، ص 868، بند 404.

يصدر حكمين نهائيين من كلتا الجهتين متناقضين. فالمرجع في ذلك مانصت عليه المادة الرابعة والسبعين في فقرته الثانية فقرة ب/إذا كان التدافع بين محكمة وجهة قضائية أخرى فيطبق بشأنه مقتضى المادتين (28 29) من نظام القضاء الصادر عام 1395هـ ونص المادتين كالتالي:

المادة 28 - إذا دفعت قضية مرفوعة أمام المحكمة بدفع يُثير نزاعاً تختص بالفصل فيه جهة قضاء أخرى وجب على المحكمة إذا رأت ضرورة الفصل في الدفع قبل الحكم في موضوع الدعوى أن توقفها وتُحدِّد للخصم الموجَّه إليه الدفع ميعاداً يستصدر في حكماً نهائياً من الجهة المختصة. فإن لم ترَ لزوماً لذلك أغفلت موضوع الدفع وحكمت في موضوع الدعوى وإذا قصر الخصم في استصدار حكم نهائي في الدفع في المدة المحدد كان للمحكمة أن تفصل في الدعوى بحالتها.

مادة 29 - إذا رفعت دعوى عن موضوع واحد أمام إحدى المحاكم الخاضعة لهذا النظام وأمام أية جهة أخرى تختص بالفصل في بعض المنازعات ولم تتخلَ إحداهما عن نظرها أو تخلت كلتاهما يرفع طلب تعيين الجهة المختصة إلى لجنة تنازع الاختصاص التي تؤلف من ثلاثة أعضاء عضوين من أعضاء مجلس القضاء الأعلى المتفرغين يختارهما مجلس القضاء الأعلى ويكون أقدمهما رئيساً. والثالث رئيس الجهة الأخرى أو مَن يُنيبه كما تختص هذه اللجنة بالفصل في النزاع الذي يقوم بشأن تنفيذ حكمين نهائيين متناقضين صادر احدهما من إحدى المحاكم الخاضعة لهذا النظام والآخر من الجهة الأخرى[1].

ويمكن التعويل على القواعد العامة للطعن في الأحكام باعتبارها الطريق الطبيعي المتاح للطعن على الأحكام، فيكون لذوي الشأن الطعن في الحكم الصادر من إحدى المحكمتين في مسألة الاختصاص وفقاً لنظام الطعن

---

(1) نظام المرافعات الشرعيةالصادر بالمرسوم الملكي م/21 وتاريخ 1421/5/20هـ. نظام القضاء الصادر بالمرسوم الملكي م/64 وتاريخ1395/7/14هـ.

في الأحكام ويمكن إبداء الملاحظات الآتية في شأن التنازع وطرق الطعن التي يمكن ولوجها لحله:

1 – أن إعمال نص المادة (74) من النظام التي تلزم المحكمة إذا قررت عدم اختصاصها بالدعوى أن تعين المحكمة المختصة، وأن تُحيل إليها مع إلزام المحكمة المحال إليها بما يتقرَّر في حكم الإحالة بشأن اختصاصها، يجعل حالات التنازع السلبي على الاختصاص نادرة في العمل.

2 – الأحكام الصادرة بالاختصاص لا تقبل الطعن المباشر وعلى استقلال، وإنما يكون الطعن فيها بعد صدور الحكم الختامي المنهي للخصومة (م/175) أما الأحكام الصادرة بعدم الاختصاص والإحالة فإنها تقبل الطعن المباشر وعلى استقلال.

3 – تقبل الأحكام الصادرة بالمخالفة لقواعد الاختصاص الطعن فيها وإحالتها إلى محكمة التمييز لمخالفتها لقواعد الاختصاص، وفي حالة قبول الطعن ونقض الحكم، فإن محكمة (التمييز) تعين المحكمة المختصة التي يجب التداعي إليها بإجراءات جديدة (م/188).

ويقتصر الفصل من جانب هذه المحكمة على بحث مسألة الاختصاص فقط (م/186).

المطلب الثاني

الجهة المختصة بنظر الجرائم المعلوماتية في النظام السعودي

مراكز الشرطة في المملكة العربية السعودية هي الجهة المختصة باستقبال هذا النوع من الطلبات وما شابهها مما قد يُمثِّل جريمة معلوماتية مشمولة في نظام مكافحة جرائم المعلوماتية الصادر بتاريخ 1428/3/8هـ،

والجهة المسئولة في المملكة العربية السعودية هي اللجنة الأمنية الدائمة للانترنت والتي تم تشكيلها بموجب قرار مجلس وزراء رقم ١٦٣ وتاريخ 1417/10/24هـ والذي تضمن إدخال الانترنت للمملكة، وهذه اللجنة برئاسة وزارة الداخلية وعضوية جهات متعددة من بينها هيئة الاتصالات وتقنية المعلومات وينحصر دور هيئة الاتصالات وتقنية المعلومات بناء على ما ورد في قرار مجلس الوزراء رقم ٢٢٩ وتاريخ 1425/8/13هـ وحسب توجيهات اللجنة الأمنية الدائمة فيما يلي:

1 - استقبال التوجيهات من الجهات المعنية وتنفيذها، وكذلك استقبال طلبات الحجب ورفع الحجب من عموم المستخدمين.

2 - الإشراف على الشركات والجهات المقدمة لخدمة الانترنت والتأكد من التزامهم بمتطلبات الترشيح.

3 - وضع التصورات التقنية والتنظيمية لترشيح خدمات الانترنت بالتنسيق مع الجهات المعنية.

4 - حجب المواقع الإباحية والمواقع التي توفر وسائل لتجاوز الترشيح وإحالة ما عدا ذلك إلى اللجنة الأمنية الدائمة للانترنت.

وتستقبل الهيئة جميع طلبات الحجب الواردة من عموم المستخدمين باستثناء الطلبات التالية:

1 - الطلبات المتعلقة بالقبائل والأسر حيث أن الجهة المختصة باستقبال الطلبات هي إمارة المنطقة التي يتبع لها صاحب الشكوى.

2 - الطلبات المتعلقة بأمور (القذف)، (والسب)، (والشتم) المنصوص عليها في نظام مكافحة جرائم المعلوماتية، فيتم التقدم ببلاغ إلى الجهات الأمنية (مركز الشرطة).

3 – الطلبات المتعلّقة بتقليد شعار أو علامة تجارية مسجلة حيث أن الجهة المختصة باستقبال الطلبات هي وزارة التجارة والصناعة.

4 – الطلبات المتعلقة بالنشر الإليكتروني وحقوق الملكية الفكرية حيث أن الجهة المختصة باستقبال الطلبات هي وزارة الثقافة والإعلام.

أما بخصوص طلبات رفع الحجب فيتم استقبال الطلبات ومن ثم إحالتها إلى جهة الاختصاص. فينظر في جميع الطلبات التي يرسلها المستخدمون للحجب وإلغاء الحجب وينظر إلى كل طلب، فكل طلب يرسل من قِبل المستخدم يتم إنشاء تذكرة خاصة بكل رابط مذكور في الطلب ومن ثم يتم إحالتها إلى الفريق المختص في الهيئة لدراسة الموقع واتخاذ الإجراء المناسب حياله. وفي ما يخص المواقع الإباحية فدور الهيئة يتمثّل بمنع الوصول إليها، أما ما يتعلّق بمقاضاة أصحابها فقد نص نظام الجرائم المعلوماتية في المادة السادسة على تجريم أمثال هؤلاء، وحسب النظام فإن الجهات الأمنية (مراكز الشرطة) هي الجهة المختصة بضبط وتلقي البلاغات ذات العلاقة بهذه الجرائم وأمثالها والتي ورد النص عليه في نظام الجرائم المعلوماتية، كما أن الهيئة تقوم بإحالة الروابط التي قد تُمثّل جريمة معلوماتية إلى الجهة الأمنية المختصة. ويتم التعامل مع جميع الاستفسارات والطلبات والاتصالات فالفريق المختص يبذل قصارى جهده للتعامل مع الطلبات الواردة من المستخدمين (طلبات حجب، رفع حجب، استفسارات، مكالمات)، علماً أنه يرد للهيئة ما معدله 2500 طلب يومياً، كما أن أوقات العمل للفريق هي أوقات الدوام الرسمي في الهيئة (من السبت إلى الأربعاء، في الفترة من الساعة 7:30 ص إلى الساعة 3:30 مساءً والمدة التي تستغرقها معالجة الطلبات: يتم النظر في الطلبات خلال مدة لا تزيد عن يومي عمل ومن ثم اتخاذ الإجراء المناسب، وقد يتأخر اتخاذ القرار إما بسبب الحاجة لإحالة الطلب لجهة الاختصاص أو لكون الموقع يحتاج إلى مزيد دراسة وفحص.

المطلب الثالث

الاختصاص الجنائي للمحكمة الرقمية

تختص المحكمة الرقمية جنائياً بالعقاب على كافة الجرائم المعلوماتية باختلاف أنواعها وأشكالها فالجريمة المعلوماتية إن كان يصعب الاتفاق على تعريف موحَّد لها، حيث اختلفت الاجتهادات في ذلك اختلافاً كبيراً، ويرجع ذلك إلى سرعة وتيرة تطور التقنية المعلوماتية من جهة، وتباين الدور الذي تلعبه هذه التقنية في الجريمة من جهة أخرى، فالنظام المعلوماتي لهذه التقنية يكون محلاً للجريمة تارة، ويكون وسيلة لارتكابها تارة أخرى، فكلما كان البحث منصباً على الجرائم التي ترتكب ضد النظام المعلوماتي انطلق التعريف من زاوية محل الجريمة بأنها الجريمة المرتكبة بالاعتداء على النظام المعلوماتي، أما إذا كان البحث منصباً على دراسة الجرائم التي ترتكب باستخدام التقنية المعلوماتية ارتكز التعريف على الوسيلة وكان: «كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب الآلي [1]. تجد الإشارة أيضاً إلى أن أهم عوامل صعوبة الاتفاق على تعريف هو أن التقنية المعلوماتية أصبحت تحل محل العديد من التقنيات السابقة كالهاتف والفاكس والتلفزيون، فالمسألة لم تقتصر على معالجة البيانات فحسب تعدتها إلى وظائف عديدة مثل وظيفة النشر والنسخ، وهو ما يحتم ضرورة التفرقة بين جرائم الإنترنت وشبكات المعلومات بالمعنى الفني عن بقية الجرائم الأخرى التي يستخدم فيها الانترنت أو الحاسب الآلي كأداة لارتكابها. فيقصد بجرائم الانترنت وشبكات المعلومات الدخول غير المشروع إلى الشبكات الخاصة كالشركات والبنوك وغيرها وكذلك الأفراد، والعبث بالبيانات الرقمية التي تحتويها شبكة المعلومات مثل تزييف البيانات أو إتلافها ومحوها، وامتلاك

(1) رستم، هشام محمد فريد، قانون العقوبات ومخاطر تقنية المعلومات، الطبعة الأولى، مكتبة الآلات الحديثة، اسيوط، 1992م.

أدوات أو كلمات سرية لتسهيل ارتكاب مثل هذه الجرائم التي تلحق ضرراً بالبيانات والمعلومات ذاتها وكذلك بالنسبة للبرامج والأجهزة التي تحتويها وهي الجرائم التي تلعب فيها التقنية المعلوماتية دوراً رئيسياً في مادياتها أو السلوك الإجرامي فيها. أما الجرائم التقليدية الأخرى مثل غسيل الأموال، تجارة المخدرات، الإرهاب، الدعارة [1]، الاستخدام غير المشروع للكروت الإليكترونية، ودعارة الأطفال وجرائم التجارة الإليكترونية، وكذلك جرائم السب والقذف، هي جرائم تستخدم التقنية المعلوماتية كأداة في ارتكابها دون أن تكون جرائم معلوماتية بالمعنى الفني وإن كان يطلق عليها الجرائم الإليكترونية [2].

نصل إلى أن الجرائم المعلوماتية لها أنواع وأصناف عديدة، وكما أسلفنا القول فإن الجريمة المعلوماتية تتميز بأنها تضم نوعين من الجرائم المستحدثة، الأول أنواعاً مستحدَثة من الاعتداء على مصالح محمية جنائياً بالنصوص القانونية التقليدية، أي أن في هذه الحالات فإن طرق الاعتداء فقط هي المستحدثة لأنها تتم عن طريق التقنية المعلوماتية بعد أن كانت ترتكب بالسلوك المادي الملموس، أما محل الاعتداء فهي المصالح المحمية أصلاً حماية جنائية على مر الأزمان والعصور كالأموال والشرف والاعتبار، أما النوع الثاني فيضم أنواعاً أخرى من الاعتداءات بالطرق المستحدثة على مصالح مستحدثة لم تعرفها القواعد التقليدية كالشبكات المعلوماتية التي تتعرُض للاختراق أو التعطل أو الإغراق [3].

---

(1) الكركي، كمال، جرائم الحاسوب ودور مديرية الأمن في مكافحتها، ورقة عمل مقدمة إلى ندوة قانون حماية حق المؤلف، نظرة إلى المستقبل، المنعقدة في عمان بتاريخ 1999/7/5م.

(2) البربري، صالح أحمد، دور الشرطة في مكافحة جرائم الإنترنت في إطار الاتفاقية الأوروبية، الموقعة في بودابست في 2001/11/23، www. arablawinfo. com، ص2.

(3) اغراق الشبكة بالرسائل والمعلومات لاستنفاذ سعتها ومن ثم تعطيلها.

المبحث الرابع

الاختصاص بنظر الجريمة المعلوماتية

في ظل لامركزية القضاء وعالمية الجريمة المعلوماتية فقدت الحدود الجغرافية كل أثر لها في الفضاء الشبكي أو الآلي، فلا يعترف بالحدود الجغرافية حيث يتم تبادل البيانات في شكل حزم إليكترونية توجه إلى عنوان افتراضي ليس له صلة بالمكان الجغرافي، فهو فضاء ذو طبيعة لا مركزية ويمكن إجمال أهم خصائصه في عدم التبعية لأي سلطة حاكمة. فالفضاء الآلي: نظام إليكتروني معقد لأنه عبارة عن شبكة اتصال لا متناهية غير مجسدة وغير مرئية متاحة لأي شخص حول العالم وغير تابعة لأي سلطة حاكمة فالسلوك المرتكب فيها يتجاوز الأماكن بمعناه التقليدي له وجود حقيقي وواقعي لكنه غير محدد المكان لكنه حقيقة واقعاً [1].

فالشبكة عالمية النشاط والخدمات لا تخضع لأي قوة مهيمنة إلا في بدايتها حيث كان تمويل هذه الشبكة حكومياً يعتمد على المؤسسة العسكرية الأمريكية، أما الآن فقد أصبح التمويل يأتي من القطاع الخاص حيث الشركات الإقليمية ذات الغرض التجاري التي تبحث عن كافة السبل للاستفادة من خدماتها بمقابل مالي [2].

والجريمة المعلوماتية جريمة تعبر الحدود والقارات، وهو ما يدرجها ضمن موضوعات القانون الجنائي الدولي، الذي يقابل القانون الدولي الخاص في القانون المدني، وهو ذلك الفرع من القانون الذي يحدد ضوابط

---

(1) مصلح، يحيى، التجارة على الانترنت. سايمون كولن، نقله إلى العربية، بيت الأفكار الدولية بأمريكا 1999م.

(2) الجنبيهي، منير، والجنبيهي، ممدوح، صراخ الانترنت وسائل مكافحتها، 2005 م، دار الفكر الجامعي، الإسكندرية، ص 9.

مجالات التعاون الدولي في مجال مكافحة الجريمة بالتزام الدول الموقعة على الاتفاقيات بالعمل بمقتضاها في مكافحة الجريمة [1].

وقد ازدادت أهمية القانون الجنائي الدولي بعدما تطورت الجريمة المنظمة في وقت تقلص فيه المفهوم التقليدي للسيادة، حيث اتسع نظام المعاهدات الدولية لمكافحة الجرائم العابرة للحدود فالجانب الدولي للجريمة المعلوماتية لا يعد عنصراً من عناصرها كما هو الحال في الجريمة الدولية بل يعد هو نطاقها المكاني.

أن القواعد العامة التي تحكم نطاق تطبيق النصوص الجنائية - التي تتمثّل في مبدأ إقليمية النص الجنائي والاستثناءات الواردة عليه - تقتضي تطبيق النص الجنائي على كل الجرائم الواقعة في إقليمه، إلا في أحوال خاصة نص عليها المشرع في المواد 4 وما بعدها تبين حالات يطبق فيها القانون الليبي على جرائم ارتكبت خارج إقليمه.

ويعتمد النظام القانوني السابق على جريمة ترتكب في مكان قابل للتحديد الجغرافي، أما الجريمة المعلوماتية فهي جريمة تُرتكب في مسرح غير قابل للتحديد الجغرافي، إلا أنه يضم اكبر تجمع إنساني يتميز بارتباط وتشابك معقد، وتتمثّل أهم خصائصه في خلق آليات خاصة لفرض الالتزامات والإذعان لها مثل قطع الاتصال على مخترقي بعض القواعد أو طردهم من المنتديات، لكن هذا التجمع الإنساني الضخم يفتقر إلى المعايير الأخلاقية المشتركة [2].

مما حدا المجلس الأوروبي إلى عقد اتفاقية بوداست COUNCIL السابق الإشارة إليها، والتي قدمت صوراً لمكافحة هذه الجرائم ونصت المادة

(1) الشاذلي فتوح، القانون الدولي الجنائي، دار المطبوعات الجامعية، الاسكندرية، 2001، ص 34

(2) عرب، يونس، جرائم الكمبيوتر والانترنيت، المركز العربي للدراسات والبحوث الجنائية، ابو ظبي 10-2002/2/12م.

22 منها على: «أن لكل طرف اتخاذ الإجراءات التشريعية وغيرها التي يراها لازمة لكي يحدد اختصاصه بالنسبة لكل جريمة تقع وفقاً لما هو وارد في المواد من 2 إلى 11 من الاتفاقية الحالية عندما تقع الجريمة:

أ - داخل النطاق المحلي للدولة.

ب - على ظهر سفينة تحمل علم تلك الدولة.

ج - على متن طائرة مسجلة في هذه الدولة.

د - بواسطة أحد رعاياها، إذا كانت الجريمة معاقباً عليها جنائياً في المكان الذي ارتكبت فيه أو إذا كانت الجريمة لا تدخل في أي اختصاص مكاني لأي دولة أخرى.

ولكل طرف أن يحتفظ لنفسه بالحق في عدم تطبيق، أو عدم التطبيق إلا في حالات وفي ظل شروط خاصة، قواعد الاختصاص المنصوص عليها في الفقرة الأولى (ب ود) من هذه المادة أو في أي جزء من هذه الفقرات [1].

وتنص الفقرة 4 من المادة على عدم استبعاد أي اختصاص ينعقد للقضاء الوطني طبقاً للقانون المحلي الفقرة 5 تنص على أنه في حالة حدوث تنازع في الاختصاص فإنه يجب أن يتم حله بالتشاور بين الدول الاطراف حول المكان الأكثر ملائمة. كما أفردت الاتفاقية بنداً خاصاً لضرورة التعاون بين الدول.

ولم ينص القانون العربي النموذجي بشان الجرائم المعلوماتية على أي قواعد لتحديد الاختصاص بنظر هذه الجرائم. فإن كان الفقه الجنائي اليوم قبل فكرة تطبيق القانون الأجنبي لمواجهة الجريمة عبر الوطنية ما أظهر ضرورة تجاوز فكرة تلازم الاختصاص الجنائي القضائي والتشريعي فيلزم من

(1) سلامة، محمد عبد الله أبو بكر، جرائم الكومبيوتر والانترنت موسوعة جرائم المعلوماتية، المرجع السابق.

باب أولى قبول هذه الفكرة والتوسع فيها بالنسبة لجرائم ترتكب في الفضاء السيبراني الذي يتجاوز الحدود والقارات، وبذلك نصل إلى ضرورة التفكير في وضع ضوابط إسناد جنائية لتحديد الاختصاص الموضوعي والإجرامي بعد أن تصنف إلى فئات مختلفة تُشكل كل فئة فكرة مسندة تتضمن المصالح الواجب حمايتها جنائياً على المستوى العالمي لوضع ضوابط إسناد تشير إلى القانون الواجب التطبيق [1].

إلا أن هذه القواعد يجب أن تتم صياغتها في إطار اتفاقات دولية لأن الجريمة الدولية لا يمكن مواجهتها إلا بالتعاون الدولي، وهو أهم ما جاء في اتفاقية بودابست بشكل يسمح بتبادل التعاون سواء كان ذلك على مستوى جمع الأدلة أو تسليم المجرمين وهو ما يعني أن المجتمع الدولي مقبلاً على توسع في مجال التعاون القضائي الذي يتوقع أن يتم بين الأجهزة القضائية والأمنية بشكل مباشر نظراً لأن عامل الوقت في حفظ الأدلة المعلوماتية سوف يكون حرجاً ومتطلباً لسرعة الانجاز [2].

---

(1) اللحيدان، فهد بن عبدالله، الانترنت، شبكة المعلومات العالمية، الطبعة الأولى، الناشر غير معروف، 1996م.

(2) الشاذلي، فتوح، القانون الدولي الجنائي، المرجع السابق.

المبحث الخامس
الجرائم المعلوماتية من منظور شرعي وقانوني

يمكن النظر للانترنت كمهدد للأمن الاجتماعي وخاصة في المجتمعات المغلقة، حيث أن تعرُّض مثل هذه المجتمعات لقيم وسلوكيات المجتمعات الأخرى قد تسبب تلوثاً ثقافياً يؤدي إلى تفسُّخ اجتماعي وانهيار في النظام الاجتماعي العام لهذه المجتمعات. إن الاستخدام غير الأخلاقي وغير القانوني للشبكة قد يصل إلى مئات المراهقين والهواة مما يؤثر سلباً على نمو شخصياتهم النمو السليم ويوقعهم في أزمات نمو، وأزمات قيمية لا تتماشى مع النظام الاجتماعي السائد، وبخاصة عند التعامل مع المواضيع الجنسية وتقديم الصور، والمواد الإباحية، والمخاطر الأمنية متجددة وليست قاصرة على وقت أو نوع معين، و مع دخول الكمبيوتر الذكي إلى المنازل، فإن ذلك سيفتح الباب لأنواع متطورة من الجرائم التي تستغل إمكانية برمجة الأجهزة المنزلية ووصلها بالحاسب الآلي وبشبكة الانترنت، فطالما انك تستطيع مثلاً وصْل خزانة الأموال في مكتبك بشبكة الانترنت لإعطاء إنذار عند محاولة فتحها فربما يكون من الممكن فتحها عن بعد بواسطة الحاسب الآلي، ثم الوصول إليها وإفراغها ،واستلزم التطور التقني تطوُّر في طرق إثبات الجريمة والتعامل معها، فالجرائم العادية يسهل – غالباً – تحديد مكان ارتكابها، بل إن ذلك يُعتبر خطوة أولى وأساسية لكشف ملابسات الجريمة، في حين أنه من الصعوبة بمكان تحديد مكان وقوع الحادثة عند التعامل مع جرائم الانترنت، لكون الرسائل والملفات الحاسوبية تنتقل من نظام إلى آخر في ثواني قليلة، كما أنه لا يقف أمام تنقل الملفات والرسائل الحاسوبية أي حدود دولية أو جغرافية. ونتيجة لذلك فإن تحديد أين تكون المحاكمة وما هي القوانين التي تخضع لها أمر في غاية الحساسية والتعقيد خاصة وإن كل دولة تختلف قوانينها عن الدولة الأخرى، فما يعتبر جريمة في الصين مثلاً قد لا يُعتبر جريمة في أمريكا والعكس صحيح، بل إن الأمر يصل إلى حد اختلاف قوانين الولايات المختلفة داخل الدولة الواحدة كما في الولايات المتحدة الأمريكية [1].

---

(1) صدق، عبد الرحيم، الإرهاب السياسي والقانون الجنائي، دار النهضة العربية، القاهرة، 1985م.

وأدّى التطور التقني إلى ظهور جرائم جديدة لم يتناولها القانون الجنائي التقليدي، مما أجمع معه مشرِّعي القانون الوضعي في الدول المتقدمة على جسامة الجريمة المعلوماتية والتهديدات التي يمكن أن تنشأ عن استخدام الحاسب الآلي وشبكة الانترنت، ودفعهم هذا إلى دراسة هذه الظاهرة الإجرامية الجديدة وما أثارته من مشكلات قانونية حول تطبيق القانون الجنائي من حيث الاختصاص القضائي ومكان وزمان ارتكاب الجريمة؛ حيث يسهل على المجرم في مثل هذه الجرائم ارتكاب جريمة ما في مكان غير المكان الذي يتواجد فيه أو الذي حدثت فيه نتائج فعله [1]. وتطوير القوانين الجنائية وتحديثها أمر يستغرق بعض الوقت فهناك تعديلات كثيرة مطلوب إدخالها على التشريعات التي تتعامل مع الجريمة كي تأخذ في الاعتبار المعطيات الجديدة التي نشأت عن استخدام الحاسب الآلي في مجال المعلومات وعن ظهور شبكات المعلومات العالمية» [2]. ولاقت جرائم الحاسب الآلي اهتماماً عالمياً، فعقدت المؤتمرات والندوات المختلفة ومن ذلك المؤتمر السادس للجمعية المصرية للقانون الجنائي عام (1993م) الذي تناول موضوع جرائم الحاسب الآلي والجرائم الأخرى في مجال تكنولوجيا المعلومات وتوصَّل إلى توصيات أحاطت بجوانب مشكلة جرائم الحاسب الآلي إلا أنها لم تتعرَّض لجزئية هامة وهي التعاون الدولي الذي يُعتبر ركيزة أساسية عند التعامل مع هذه النوعية من الجرائم [3]. وهذا المؤتمر يُعتبر تحضيراً للمؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات الذي عُقِد في البرازيل عام (1994م) والذي وضع توصيات حول جرائم الحاسب الآلي والانترنت، والتحقيق فيها ومراقبتها وضبطها، وركَّز على ضرورة إدخال بعض التعديلات في القوانين

(1) عرب، يونس، جرائم الكمبيوتر والانترنت، المركز العربي للدراسات والبحوث الجنائية، ابو ظبي 10-2002/2/12م.

(2) غاري، ج. بيتر، ثقافة الحاسوب، الوعي والتطبيق والبرمجة، الطبعة الأولى، ترجمة ونشر مؤسسة الأبحاث اللغوية، نيقوسيا، 1987م.

(3) عوض، محمد محيي الدين، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، المنعقد بالقاهرة في الفترة من 25 – 28 أكتوبر 1993م.

الجنائية لتواكب مستجدات هذه الجريمة وافرازاتها [1]. والتعاون الدولي مهم عند التعامل مع جرائم الانترنت، كونه سيطوِّر أساليب متشابهة لتحقيق قانون جنائي وإجرائي لحماية شبكات المعلومات الدولية، خاصة أن هذه الجرائم هي عابرة للقارات ولا حدود لها، وفي المقابل فإن عدم التعاون الدولي سيؤدي إلى زيادة القيود على تبادل المعلومات عبر حدود الدول مما سيعطي الفرصة للمجرمين من الإفلات من العقوبة ومضاعفة أنشطتهم الإجرامية [2].

وتطبِّق كندا قوانين متخصصة ومفصَّلة للتعامل مع جرائم الحاسب الآلي والانترنت؛ حيث عدَّلت في عام (1985م) قانونها الجنائي بحيث شمل قوانين خاصة بجرائم الحاسب الآلي والانترنت، كما شمل القانون الجديد تحديد عقوبات المخالفات الحاسبية، وجرائم التدمير، أو الدخول غير المشروع لأنظمة الحاسب الآلي، كما وضَّح فيه صلاحيات جهات التحقيق كما جاء في قانون المنافسة (The Competition Act) مثلاً الذي يخول لمأمور الضبط القضائي متى ما حصل على أمر قضائي حق تفتيش أنظمة الحاسب الآلي والتعامل معها وضبطها [3]. 255) **أنظمة قضائية المادة الأولى:** يُقصد بالألفاظ والعبارات الآتية أينما وردت في هذا النظام المعاني المبينة أمامها ما لم يقتضِ السياق خلاف ذلك:

1 - الشخص: أي شخص ذي صفة طبيعية أو اعتبارية، عامة أو خاصة.

---

(1) Donn B. Parker, Fighting Computer Crime: A New Framework for Protecting Information, 1 edition, John Wiley & Sons 1998.

(2) عرب، يونس، جرائم الكمبيوتر والانترنت، المركز العربي للدراسات والبحوث الجنائية، ابو ظبي 10-12/2/2002م.

(3) الطويل، خالد بن محمد، التعامل مع الاعتداءات الإليكترونية من الناحية الأمنية مركز المعلومات الوطني، وزارة الداخلية، ورقة عمل مقدمة لورشة العمل الثالثة (أحكام في المعلوماتية) الذي نظمه مشروع الخطة الوطنية لتقنية المعلومات 1423/10/19هـ الرياض.

2 - النظام المعلوماتي: مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها، وتشمل الحاسبات الآلية.

3 - الشبكة المعلوماتية: ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول على البيانات وتبادلها، مثل الشبكات الخاصة والعامة والشبكة العالمية.

4 - البيانات: المعلومات، أو الأوامر، أو الرسائل، أو الأصوات، أو الصور التي تُعد، أو التي سبق إعدادها، لاستخدامها في الحاسب الآلي، وكل ما يمكن تخزينه، ومعالجته، ونقله، وإنشاؤه بوساطة الحاسب الآلي، كالأرقام والحروف والرموز وغيرها.

5 - برامج الحاسب الآلي: مجموعة من الأوامر، والبيانات التي تتضمّن توجيهات أو تطبيقات حين تشغيلها في الحاسب الآلي، أو شبكات الحاسب الآلي، وتقوم بأداء الوظيفة المطلوبة.

6 - الحاسب الآلي: أي جهاز إليكتروني ثابت، أو منقول سلكي، أو لاسلكي، يحتوي على نظام معالجة البيانات، أو تخزينها، أو إرسالها، أو استقبالها، أو تصفحها، يؤدي وظائف محددة بحسب البرامج، والأوامر المعطاة له.

7 - الدخول غير المشروع: دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع إليكتروني أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرَّح لذلك الشخص بالدخول إليها.

8 - الجريمة المعلوماتية: أي فعل يُرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام.

9 - الموقع الإليكتروني: مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد.

10 - الالتقاط: مشاهدة البيانات، أو الحصول عليها دون مسوّغ نظامي صحيح.

المادة الثانية: يهدُف هذا النظام إلى الحد من وقوع جرائم المعلوماتية، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها، وبما يؤدي إلى ما يأتي:

1 - المساعدة على تحقيق الأمن المعلوماتي.

2 - حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية.

3 - حماية المصلحة العامة، والأخلاق، والآداب العامة.

4 - حماية الاقتصاد الوطني.

المادة الثالثة: يُعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

1 - التصنُّت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي دون مسوّغ نظام صحيح أو التقاطه أو اعتراضه.

2 - الدخول غير المشروع لتهديد شخص أو ابتزازه، لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً.

3 - الدخول غير المشروع إلى موقع إليكتروني، أو الدخول إلى موقع إليكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه.

4 - المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزوّدة بالكاميرا، أو ما في حكمها.

5 - التشهير بالآخرين، وإلحاق الضرر بهم، عبر وسائل تقنيات المعلومات المختلفة.

المادة الرابعة: يُعاقب بالسجن مدة لا تزيد عن ثلاث سنوات وبغرامة لا تزيد على مليوني جنيه، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

1 - الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة.

2 - الوصول دون مسوِّغ نظام صحيح إلى بيانات بنكية أو ائتمانية، أو بيانات متعلِّقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تُتيحه من خدمات.

المادة الخامسة: يُعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين جنيه، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

1 - الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها.

2 - إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدميرها، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها.

3 - إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت.

المادة السادسة: يُعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين جنيه، أو بإحدى هاتين العقوبتين، كل

شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

1 - إنتاج ما من شأنه المساس بالنظام العام، أو القيم الدينية، أو الآداب العامة، أو حرمة الحياة الخاصة، أو إعداده، أو إرساله، أو تخزينه عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي.

2 - إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره للاتجار في الجنس البشري، أو تسهيل التعامل به.

3 - إنشاء المواد والبيانات المتعلّقة بالشبكات الإباحية، أو أنشطة الميسر المخلة بالآداب العامة، أو نشرها، أو ترويجها.

4 - إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، للاتجار بالمخدرات أو المؤثرات العقلية، أو ترويجها، أو طرق تعاطيها، أو تسهيل التعامل بها.

المادة السابعة: يُعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين جنيه، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

1 - إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أي أداة تستخدم في الأعمال الإرهابية.

2 - الدخول غير المشروع إلى موقع إليكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمسُّ الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني.

المادة الثامنة: لا تقل عقوبة السجن أو الغرامة عن نصف حدها الأعلى إذا اقترنت الجريمة بأي من الحالات الآتية:

1 - ارتكاب الجاني الجريمة من خلال عصابة منظمة.

2 - شغل الجاني وظيفة عامة، واتصال الجريمة بهذه الوظيفة، أو ارتكابه الجريمة مستغلاً سلطاته أو نفوذه.

3 - التغرير بالقصَّر ومَن في حكمهم، واستغلالهم.

4 - صدور أحكام محلية أو أجنبية سابقة بالإدانة بحق الجاني في جرائم مماثلة.

المادة التاسعة: يُعاقب كل مَن حرَّض غيره، أو ساعده، أو اتفق معه على ارتكاب أي من الجرائم المنصوص عليها في هذا النظام؛ إذا وقعت الجريمة بناء على هذا التحريض، أو المساعدة، أو الاتفاق، بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها، ويُعاقب بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة لها إذا لم تقع الجريمة الأصلية.

المادة العاشرة: يُعاقب كل مَن شرع في القيام بأي من الجرائم المنصوص عليها في هذا النظام بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة.

المادة الحادية عشرة: للمحكمة المختصة أن تعفي من هذه العقوبات كل مَن يُبادر من الجناة بإبلاغ السلطة المختصة بالجريمة قبل العلم بها وقبل وقوع الضرر، وإن كان الإبلاغ بعد العلم بالجريمة تعين للإعفاء أن يكون من شأن الإبلاغ ضبط باقي الجناة في حال تعددهم، أو الأدوات المستخدمة في الجريمة.

المادة الثانية عشرة: لا يخل تطبيق هذا النظام بالأحكام الواردة في الأنظمة ذات العلاقة وخاصة ما يتعلّق بحقوق الملكية الفكرية، والاتفاقيات الدولية ذات الصلة التي تكون المملكة طرفاً فيها.

المادة الثالثة عشرة: مع عدم الإخلال بحقوق حسني النية، يجوز الحكم بمصادرة الأجهزة، أو البرامج أو الوسائل المستخدَمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام، أو الأموال المحصلة منها. كما يجوز الحكم بإغلاق الموقع الإليكتروني، أو مكان تقديم الخدمة إغلاقاً نهائياً أو مؤقتاً متى كان مصدراً لارتكاب أي من هذه الجرائم، وكانت الجريمة قد ارتكبت بعلم مالكه.

المادة الرابعة عشرة: يتولى الجهاز القومي للاتصالات وفقاً لاختصاصه تقديم الدعم والمساندة الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة.

المادة الخامسة عشرة: تتولى النيابة العامة التحقيق والادعاء في الجرائم الواردة في هذا النظام.

المادة السادسة عشرة: يُنشر هذا القانون في الجريدة الرسمية ويُعمل به فور نشره.

وفي عام (1985م) سنَّت الدنمارك أول قوانينها الخاصة بجرائم الحاسب الآلي والانترنت، والتي شملت في فقراتها العقوبات المحددة لجرائم الحاسب الآلي كالدخول غير المشروع إلى الحاسب الآلي أو التزوير أو أي كسب غير مشروع سواء للجاني أو لطرف ثالث أو التلاعب غير المشروع ببيانات الحاسب الآلي كإتلافها أو تغييرها أو الاستفادة منها [1]. وكانت فرنسا من الدول التي اهتمت بتطوير قوانينها الجنائية للتوافق مع المستجدات الإجرامية حيث أصدرت في عام (1988م) القانون رقم (19-88) الذي أضاف إلى قانون العقوبات الجنائي جرائم الحاسب الآلي والعقوبات المقررة لها، كما تم عام (1994م) تعديل قانون العقوبات لديها ليشمل مجموعة

(1) Tom Douglas Brian Loader, Thomas Douglas, Cyber crime: Law Enforcement, Security, and Surveillance in the Information Age, 1st edition, Rutledge, 2000.

جديدة من القواعد القانونية الخاصة بالجرائم المعلوماتية، وأوكل إلى النيابة العامة سلطة التحقيق فيها بما في ذلك طلب التحريات وسماع الأقوال [1]. أما في هولندا فلقاضي التحقيق الحق بإصدار أمره بالتصنُّت على شبكات الحاسب الآلي متى ما كانت هناك جريمة خطيرة، كما يُجيز القانون الفنلندي لمأمور الضبط القضائي حق التصنُّت على المكالمات الخاصة بشبكات الحاسب الآلي، كما تعطي القوانين الألمانية الحق للقاضي بإصدار أمره بمراقبة اتصالات الحاسب الآلي وتسجيلها والتعامل معها وذلك خلال مدة أقصاها ثلاثة أيام[2].

ونجد أن أنظمة وتشريعات الانترنت وهي الأنظمة العربية السعودية المستمدة من الشريعة الإسلامية تضع بعض الحواجز والروادع أمام مَن يرتكب مثل هذه الجرائم بالأفعال الآتية:

1 - منع انتحال أرقام الانترنت وهي التي يقوم خلالها بعض المتسللين المحترفين باستخدام أرقام بعض الأشخاص بطريقةٍ غير مشروعة.

2 - منع إساءة استخدام البريد الإليكتروني أو ما يُعرف سواء للتهديد أو لإرسال عروض أسعار أو دعايات لا يقبل بها المستخدم وهو ما عرف اصطلاحاً باسم البريد المهمل والذي ينتشر بشكل كبير في الدول المتقدمة.

3 - الاحتفاظ بسجل استخدام مزود الاتصال الخاص بالمشتركين وسجل استخدام البروكسي (Proxy) لمدة لا تقل عن (6) أشهر.

4 - الحصول على خدمة الوقت (NTP) عن طريق وحدة البروكسي

(1) البحر، ممدوح خليل، أصول المحاكمات الجزائية، ط1، دار الثقافة، عمان، 1998م.

(2) رستم، هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، 1994م

ومزود الاتصال بهدف اللجوء إليها لمعرفة توقيت حدوث عملية الاختراق للأجهزة أو الشبكات.

5 - تحديث سجلات منظمة رايب (www.ripe.com) الخاصة بمقدمي الخدمة.

6 - ضرورة تنفيذ ما تتوصّل إليه اللجنة الأمنية الدائمة بخصوص متابعة ومعاقبة المخالفات الأمنية.

المبحث السادس

الجريمة المعلوماتية في النظام السعودي

المطلب الأوّل

نبذة عن نظام مكافحة الجريمة المعلوماتية السعودي

أقر مجلس الوزراء السعودي يوم الاثنين 7 ربيع الأول 1428هـ نظام مكافحة الجرائم المعلوماتية رقم 79 وتاريخ 1428/3/7هـ، وتمت المصادقة عليه بموجب المرسوم الملكي الكريم رقم م/17 وتاريخ 1428/3/8هـ. ويهدُف إلى الحد من نشوء جرائم المعلوماتية وذلك بتحديد تلك الجرائم والعقوبات المقررة لها، وفرض النظام عقوبة بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال أو بإحداهما على كل شخص يرتكب أياً من الجرائم المنصوص عليها في النظام ومنها الدخول غير المشروع إلى موقع إليكتروني أو الدخول إلى موقع إليكتروني لتغيير تصاميم هذا الموقع، أو إلغائه، أو إتلافه، أو تعديله، أو شغل عنوانه، أو المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بكاميرا أو ما في حكمها بقصد التشهير بالآخرين وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة، كذلك فرض النظام عقوبة السجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال أو بإحداهما على كل شخص يُنشئ موقعاً لمنظمات إرهابية على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي أو نشره لتسهيل الاتصال بقيادات تلك المنظمات، أو ترويج أفكارها، أو نشر كيفية تصنيع المتفجرات، ومع صدور هذا النظام الذي يسعى إلى تحقيق توازن ضروري بين مصلحة المجتمع في الاستعانة بالتقنية الحديثة ومصلحة الإنسان في حماية حياته الخاصة والحفاظ على أسراره، والمساعدة على

تحقيق النظام المعلوماتي وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية، كما يهدُف إلى حماية المصلحة العامة والأخلاق والآداب العامة وكذلك حماية الاقتصاد الوطني.

ويتضمن فرض عقوبات من بينها السجن وغرامات مالية على مخربي شبكة المعلوماتية (المتسللين)، وأن العقوبات على مخربي الانترنت ستحدَّد وفقاً للضرر الناجم عن عمليات الاختراق والأعمال التخريبية، وأن العقوبة قد تصل إلى السجن سبع سنوات إلى جانب غرامات مالية. وهذه التنظيمات مفيدة ولا شك إلا أنها ليست كافية، فالمهم هنا وبداية تحديد جهة متخصصة ومؤهلة للتعامل مع جرائم الانترنت تحقيقاً وضبطاً ووقاية، خلاف مدينة الملك عبد العزيز التي تضطلع بمهام كثيرة ومختلفة عن المهام التي ستوكل للجهة التي ستحدد لمثل هذا العمل. وعلى كل حال فيجب أن لا يركن إلى الأنظمة والتعليمات فقط عند التعامل مع الجرائم والتجاوزات، فالأنظمة ليست وحدها الرادع لأي مخالفات أو سلبيات وخاصة في بيئة دينية محافظة كالمملكة العربية السعودية؛ حيث يلعب الوازع الديني والرقابة الذاتية دور مهم في عملية الردع والحد من أي تجاوزات، فمن المهم أن يؤخَذ الجانب الديني في الاعتبار عند مناقشة أخلاقيات تداول المعلومات كنوع من الضوابط الدينية التي تحكم أخلاقيات استخدام وتداول المعلومات، والتي تردع أي اتجاه لدى الأفراد نحو ارتكاب جرائم نظم المعلومات (الانترنت) [1]، فالملاحظ انه توجد معلومات تقدمها جهات كثيرة بالمجان وشبكة الانترنت متخمة بكميات هائلة من هذه المعلومات الصالح منها والمفسد. وينطبق هذا على جميع أنواع العلوم والفنون من خلال ملايين المواقع التي يطلع على محتواها أكثر من ستين إلى مائة مليون متصل بالشبكة يومياً ويتضاعف عددهم بسرعة مخيفة. ومن ثم يجب أن نركز على ضرورة وجود الضوابط الدينية والأخلاقية، فالذي لا وازع ولا ضمير له قد أتيحت له وسيلة سهلة

(1) صحيفة عكاظ السعودية عدد رقم (12789) وتاريخ1422/6/13هـ.

للغاية في توصيل أفكاره ونشر مفاسده بالدرجة نفسها المتاحة أمام النافعين للناس، وقوانين الدول تختلف فيما تتبناه من أساليب للتحكم فيما ينشر عبر شبكة الانترنت، والمحرمات تختلف من مكان لآخر»[1]. ولعلنا لا نغفل العادات والتقاليد المستوحاة من شريعتنا الإسلامية وتقاليدنا العربية الأصيلة والتي تزرع بداخل المواطن الوازع الديني الرادع عن ارتكاب المخالفات والنواهي، ومع كل هذه الضوابط فالنفس أمَّارة بالسوء والشيطان يجري من ابن ادم مجرى الدم، فيجب أن يكون هناك ضوابط عقابية تحد من يضعف رادعه الإيماني ليجد الرادع السلطاني له بالمرصاد فإن الله ليردع بالسلطان ما لا يردع بالقرآن.

وأوضح نظام مكافحة جرائم تقنية المعلومات في المملكة أغراض هذا النظام بقوله في المادة الثانية منه: «يهدُف هذا النظام إلى ضبط التعاملات والتوقيعات الإليكترونية، وتنظيمها وتوفير إطار نظامي لها بما يؤدي إلى تحقيق ما يلي:

1 – إرساء قواعد نظامية موحَّدة لاستخدام التعاملات والتوقيعات الإليكترونية، وتسهيل تطبيقها في القطاعين العام والخاص بوساطة سجلات إليكترونية يعول عليها.

2 – إضفاء الثقة في صحة التعاملات والتوقيعات والسجلات الإليكترونية وسلامتها

3 – تيسير استخدام التعاملات والتوقيعات الإليكترونية على الصعيدين المحلي والدولي للاستفادة منها في جميع المجالات، كالإجراءات الحكومية، والتجارة، والطب، والتعليم، والدفع المالي الإليكتروني.

---

(1) قايد، أسامة عبد الله، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، المرجع السابق.

4 - إزالة العوائق أمام استخدام التعاملات والتوقيعات الإليكترونية.

5 - منع إساءة الاستخدام والاحتيال في التعاملات والتوقيعات الإليكترونية».

يجمع الأفعال التي يريد العقاب عنها في خمس مجموعات متناسقة في أنه يجمعها خطورة متقاربة واعتداء على مصالح واحدة، وذلك مع مراعاة تدرج العقوبات المقررة.

المطلب الثاني

العقوبات المقررة في نظام مكافحة الجرائم المعلوماتية السعودي

تشمل المجموعة الأولى من الأفعال الدخول غير المصرَّح به، والتصنت والتشهير بالأفراد وقد قرر لها المنظِّم عقوبة أخف عن غيرها، وهي السجن الذي لا يزيد عن سنة واحدة، والغرامة التي لا تزيد على خمسمائة ألف ريال، أو إحدى هاتين العقوبتين (المادة الثالثة). فتنص المادة السابقة على أنه: «يُعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

1 - التصنت على ما هو مرسَل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي - دون مسوِّغ نظامي صحيح - أو التقاطه أو اعتراضه.

2 - الدخول غير المشروع لتهديد شخص أو ابتزازه؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه

مشروعاً.

3 - الدخول غير المشروع إلى موقع إليكتروني، أو الدخول إلى موقع إليكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه.

4 - المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها.

5 - التشهير بالآخرين، وإلحاق الضرر بهم، عبر وسائل تقنيات المعلومات المختلفة».

أما المجموعة الثانية من الأفعال فهي تتميز بتوافر خطورة متقاربة واعتداء على مصالح متناسقة، وهي الاعتداء على أموال الغير، أو تهديد أنظمة البنوك، ومن الواضح أن تلك الأنظمة تحمي أموال الغير. وقد قرر النظام عقوبة السجن مدة لا تزيد على أربع سنوات والغرامة التي لا تزيد على ثلاثة ملايين ريال، أو إحدى هاتين العقوبتين (المادة الرابعة). فتنص المادة السابقة على أنه: «يُعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

1 - الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة.

2 - الوصول - دون مسوِّغ نظامي صحيح - إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلِّقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات».

بعد ذلك قام النظام بتجميع أفعال في المجموعة الثالثة تتسم بخطورة أعلى وتتعلق بأفعال العدوان على الشبكة، أو المواقع والبيانات، والدخول

بغرض تحقيق تلك الغايات، وذلك في المادة الخامسة من هذا النظام. وقد قرر له المنظِّم عقوبة السجن مدة لا تزيد على خمس سنوات أو الغرامة التي لا تزيد على ثلاثة ملايين ريال، أو إحدى هاتين العقوبتين. فتنص المادة السابقة على أنه: «يُعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

1 - الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها، أو تغييرها، أو إعادة نشرها

2 - إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها.

3 - إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت».

وقد بيَّن النظام مجموعة الأفعال التي تتعلق بمخالفة النظام العام والآداب أو الاتجار بالمخدرات عن طريق الانترنت، ويُعاقب عليها النظام بالسجن مدة لا تزيد على خمس سنوات، والغرامة التي لا تزيد على ثلاثة ملايين ريال، أو إحدى هاتين العقوبتين. فتنص المادة السادسة من النظام على أنه: «يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

1 - إنتاج ما من شأنه المساس بالنظام العام، أو القيم الدينية، أو الآداب العامة، وحرمة الحياة الخاصة، أو إعداده، أو إرساله، أو تخزينه عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي.

2 - إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب

الآلي أو نشره، للاتجار في الجنس البشري، أو تسهيل التعامل به.

3 - إنشاء المواد والبيانات المتعلقة بالشبكة الإباحية، أو أنشطة الميسر المخلّة بالآداب العامة، أو نشرها، أو ترويجها.

4 - إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، للاتجار بالمخدرات، أو المؤثرات العقلية، أو ترويجها، أو طرق تعاطيها، أو تسهيل التعامل بها».

وأخيراً خصص المنظِّم السعودي المجموعة الخامسة لمعالجة الجرائم المتعلقة باستخدام شبكة الانترنت في جرائم الإرهاب، فنص على عقوبة السجن مدة تصل إلى عشر سنوات في هذا النوع من الجرائم والغرامة التي لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين. فتنص المادة السابعة على أنه: «يُعاقب بالسجن مدة لا تزيد على عشر سنوات، وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

1 - إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي، أو نشره لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أداة تستخدم في الأعمال الإرهابية.

2 - الدخول غير المشروع إلى موقع إليكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني.

سادساً: تشديد العقاب عند توافر بعض الظروف المشددة:

أورد نظام مكافحة جرائم المعلوماتية بعض الظروف التي من شأنها أن تُشدد العقاب عن العقوبة الأصلية المقررة لفاعل تلك الجرائم. فتنص المادة الثامنة من النظام على أنه: «لا تقل عقوبة السجن أو الغرامة عن نصف حدها الأعلى إذا اقترنت الجريمة بأي من الحالات الآتية:

1 - ارتكاب الجاني الجريمة من خلال عصابة منظمة.

2 - شغل الجاني وظيفة عامة، واتصال الجريمة بهذه الوظيفة، أو ارتكابه الجريمة مستغلاً سلطاته أو نفوذه.

3 - التغرير بالقصر ومَن في حكمهم، واستغلالهم.

4 - صدور أحكام محلية، أو أجنبية سابقة بالإدانة بحق الجاني في جرائم مماثلة».

المطلب الثالث

التحديات في تطبيق نظام مكافحة الجرائم المعلوماتية في السعودية

1 - **صعوبة الوصول إلى مرتكبي الجرائم الإليكترونية:** لأن هذه النوعية من الجرائم يمكن ارتكابها من دول أخرى في العالم، فالجاني قد يكون في دولة والمجني عليه في دولة أخرى بعكس الجرائم التقليدية.

2 - **صعوبة تعين الجاني الحقيقي:** استخدام أسماء وهمية أو انتحال شخصيات أخرى قد يحول دون الوصول إلى الجاني الحقيقي.

بالإضافة إلا أن الجاني قد يستخدم الأماكن العامة كالمقاهي لارتكاب جرائمه التي لا تتطلب الهوية الشخصية لاستخدام أجهزتها.

3 - **عدم وجود اتفاقيات وتشريعات دولية موحدة في تجريم وملاحقة مرتكبي جرائم الإليكترونية:** فاختلاف التقاليد والثقافات والديانات بين الدول العالم، يتبعه اختلاف القوانين والأنظمة في تلك الدول، لذلك نجد بعض المعلومات أو الصور التي تنشر على الانترنت قد تكون مشروعة في بلد ومجرمة في بلد آخر.

فإيجاد بعض المنظمات الدولية لمكافحة الجرائم الإليكترونية «كالإنتربول في مكافحة الجرائم التقليدية»، سيساهم بشكل كبير في تطبيق الأنظمةالجرائم. ن السعودية خاصة إذا كان الجاني من بلد آخر.

ويُعد غياب الاتفاقيات الدولية من أبرز التحديات التي تواجه الأنظمة والقوانين السعودية.

4 - عدم وجود قوى بشرية مؤهلة ولديها الخبرة والكفاءة للعمل على الأجهزة الحديثة والبرامج المتقدمة التي تساهم مراقبة وملاحقة مرتكبي هذه الجرائم.

5 - عدم وجود قوى بشرية سعودية مؤهلة لتصميم برامج شديدة التعقيد، وعالية الجودة تستطيع من خلالها مراقبة ورصد الهجمات الإليكترونية للمواقع وأجهزة حساسة في الدولة، حيث أن استيراد الأجهزة لا يغني عن وجود الحاجة لأجهزة مصنوعة محلياً؛ لأن الأجهزة أو البرامج المستوردة قد لا تطابق المعايير الملائمة للمملكة، مما قد يؤدي إلى سرقة، أو إتلاف بيانات حساسة ترتبط ببنية تحتية، أو تهديد اقتصاد الدولة.

6 - **صعوبة إيجاد أدلة ملموسة تدين الجاني:** فسرقة أو تدمير البيانات على سبيل المثال لا يمكن من خلالها العثور على دليل يُشير إلى فاعلها أو يدين مرتكبها.

7 - **عدم وجود شراكة حقيقة بين القطاع الحكومي والخاص لمكافحة ومواجهة الجريمة الإليكترونية:** فالجهات التنظيمية والقانونية بحاجة ماسة لأجهزة تقنية متطورة وقوى بشرية مؤهلة تساهم في تحديد ومعرفة الجرائم الإليكترونية، والقدرة على التعرف هوية مرتكبيها.



الفصل الثالث

صور الجريمة المعلوماتية

إذا كانت الجرائم المعلوماتية لها صور متعددة بتعدد دور التقنية المعلوماتية من جهة، وتعدد صور الجرائم التقليدية من جهة أخرى، فإن ذلك لا يعني تناول هذا الموضوع بالطريقة المدرسية التقليدية التي تتمثّل في سرد كل الجرائم التي يتناولها قانون العقوبات، بل يجب التعرض للحالات التي تُثير مشكلة في تطبيق النصوص القانونية إما لتعذُّر المطابقة بينها وبين النصوص التقليدية، أو بسبب الفراغ التشريعي لمواجهة هذه الجرائم، ولما كان المجال لايتسع للحديث عن كل أنواع الجريمة المعلوماتية فقد تخيرنا أكثرها إثارة للمشكلات القانونية، وهي جرائم الاعتداء على الحياة الخاصة وجرائم الأموال وجريمة التزوير [1].

---

(1) الكركي، كمال، جرائم الحاسوب ودور مديرية الأمن في مكافحتها، ورقة عمل مقدمة إلى ندوة قانون حماية حق المؤلف، نظرة إلى المستقبل، المنعقدة في عمان بتاريخ 1999/7/5م.

المبحث الأوّل

جرائم الاعتداء على الحياة الخاصة للأفراد عبر الانترنت

الهدف من الحديث عن موضوع جرائم الاعتداء على الحياة الخاصة عناصر ليست لتعرُّض لتلك الجرائم التي يتعذَّر علينا مواجهتها بالنصوص التقليدية، فالاعتداء عليها يتم بواسطة هذه التقنية التي أدت إلى سلب مادية السلوك، ومناقشة الحالات التي تُثير مشكلة في تطبيق النصوص التقليدية وتكشف مدى الحاجة إلى التصدي التشريعي لهذا النوع من الجرائم، وهي جرائم الاعتداء على الحياة الخاصة عبر الانترنت.

يصعب بداية حصر عناصر الحق في الحياة الخاصة، فهي تتكون من عناصر ليست محل اتفاق بين الفقهاء فيمكن القول بأنها تشمل حرمة جسم الإنسان، والمسكن، والصورة، والمحادثات، والمراسلات، والحياة المهنية [1].

أما علاقة الحياة الخاصة بالتقنية المعلوماتية، فقد ظهرت أهميتها بانتشار بنوك المعلومات في الآونه الأخيرة لخدمة أغراض متعددة وتحقيق أهداف المستخدمين في المجالات العلمية والثقافية والعسكرية [2].

وهكذا أصبحت الشبكات المعلوماتية مستودعاً خطيراً للكثير من أسرار الإنسان التي يمكن الوصول إليها بسهولة وسرعة لم تكن متاحة في ظل سائر وسائل الحفظ التقليدية فأصبحت بنوك المعلومات أهم وأخطر عناصر الحياة الخاصة للإنسان في العصر الحديث.

وقد كان ذلك في البداية بالنسبة للمعلومات التي يُدلي بها بعض

(1) عمر، ممدوح خليل، حماية الحياة الخاصة والقانون الجنائي، دار النهضة العربية، القاهرة 1983 م، ص 207.

(2) قايد، أسامة عبد الله، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، 1994 م، ص 48.

الأشخاص بإرادتهم الخاصة أثناء تعاملاتهم مع المؤسسات العامة والخاصة في البنوك والمؤسسات المالية كمؤسسات الائتمان وشركات التأمين والضمان الاجتماعي وغيرها، فالبيانات الخاصة بشخصية المستخدم يمكن الوصول إليها عن طريق زيارة بعض المواقع على شبكة المعلومات؛ لأن شبكات الاتصال تعمل من خلال بروتوكولات موحدة تساهم في نقل المعلومات بين الأجهزة وتُسمَّى هذه البروتوكولات الخاصة مثل بروتوكولات HTTP الذي يمكن عن طريقها الوصول إلى رقم جهاز الحاسب الشخصي ومكانه وبريده الإليكتروني، كما أن هناك بعض المواقع التي يؤدي الاشتراك في خدماتها إلى وضع برنامج على القرص الصلب للحاسب الشخصي، وهو ما يُسمَّى cookies وهدفه جمع معلومات عن المستخدمين. بل إن أخطر ما في استخدام هذه الشبكة يتمثل في أن كل ما يكتبه الشخص من رسائل يحفظ في أرشيف خاص يسمح بالرجوع إليه ولو بعد عشرون عاماً. ويظن الكثيرون أن الدخول باسم مستعار أو بعنوان بريدي زائف لساحات الحوار ومجموعات المناقشة قد يحميهم ويخفي هويتهم، وفي الحقيقة فإن مزود الخدمة أو يمكنه الوصول إلى كل هذه المعلومات بل ويمكنه أيضاً معرفه المواقع التي يزورها العميل [1].

فالقوانين المقارنة اهتمت بهذه المسألة واتجهت إلى تبني العديد من الضمانات التي يمكن تلخيصها في:

مبدأ الأخطار العام: وهو أن يعلم الجمهور الهيئات التي تقوم بجمع هذه البيانات وتنوع المعلومات التي تقوم بتسجيلها [2] فيجب أن تكون هناك قيود على إنشاء الأنظمة المعلوماتية المختلفة لمعالجة البيانات.

شرعية الحصول على المعلومة: يجب أن يتم الحصول على المعلومة

---

(1) عرب، يونس، جرائم الكمبيوتر والانترنيت، المركز العربي للدراسات والبحوث الجنائية، ابو ظبي 10-2002/2/12م.

(2) لويس، بدر سليمان، أثر التطور التكنولوجي مع الحريات الشخصية في النظم السياسية، رسالة الدكتوراة، حقوق القاهرة 1982م.

بطريقة تخلو من الغش والاحتيال حيث تمنع المادة 25 من القانون الفرنسي للمعلوماتية تسجيل أي معلومة إلا إذا كانت برضاء صاحب الشأن.

التناسب بين المعلومات الشخصية المسجَّلة والهدف من ذلك التسجيل، فعلى الجهة الراغبة في إقامة أي نظام معلوماتي أن تحدد الهدف من إقامته[1].

ولقد تضمَّنت بعض القوانين العربية العديد من النصوص والقواعد التي تحمي البيانات الشخصية وتفرد عقوبات على إفشاء هذا النوع من البيانات مثال ذلك الفصل العاشر من قانون التجارة الإليكترونية المصري الصادر سنة 2004 الذي نص على حماية سرية البيانات المشفرة واحترام الحق في الخصوصية، وكذلك قانون التجارة الالكترونية وقانون التجارة والمعاملات الإليكترونية في إمارة دبي الصادر سنة 2002م وقانون التجارة الإليكترونية التونسي الصادر سنة 2000م، وهو ما يعني أن المشرِّع الليبي تأخر كثيراً في اللحاق بهذا الركب، خاصة بعد أن صدر القانون العربي النموذجي لجرائم الكومبيوتر، والذي تم إعداده من قِبل اللجنة المشتركة بين المكتب التنفيذي لمؤتمر وزراء العدل العرب والمكتب التنفيذي لمؤتمر وزراء الداخلية العرب تحت رعاية جامعة الدول العربية وجرى إقراره بوصفه منهجاً استرشادياً يستعين به المشرِّع الوطني عند إعداد تشريع في جرائم المعلوماتية [2].

ونصت المادة الثالثة نظاماً مكافحة جرائم المعلوماتية السعودي رقم 79 وتاريخ 1428/3/7:

يُعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم

(1) بيومي، حجازي عبد الفتاح، صراع الكمبيوتر والانترنت، في القانون العربي النموذجي، ص 620

(2) بيومي، حجازي عبد الفتاح، صراع الكمبيوتر والانترنت، في القانون العربي النموذجي، المرجع السابق.

المعلوماتية الآتية:

1 - التصنت على ما هو مرسل عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي - دون مسوّغ نظامي صحيح - أو التقاطه أو اعتراضه.

2 - الدخول غير المشروع لتهديد شخص أو ابتزازه؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً.

3 - الدخول غير المشروع إلى موقع إليكتروني، أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه.

4 - المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها.

5 - التشهير بالآخرين، وإلحاق الضرر بهم، عبر وسائل تقنيات المعلومات المختلفة.

ونصت المادة الخامسة من نفس النظام السابق على أنه: « يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

1 - الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها.

2 - إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها أو تدمير، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها.

3 - إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت.

المبحث الثاني

جرائم الاعتداء على الأموال عبر الانترنت

كافة القوانين والأنظمة الجنائية تُجرم الاعتداء على الأموال في صوره التقليدية كالسرقة، والنصب،، وخيانة الأمانة، واختلاس الأموال العامة، فقد كان ذلك في ظل عصر لا يعرف سوى النقود الورقية، أو المعدنية، وما يحل محلها من صكوك أو أوراق مالية كالكمبيالات والسند الأذنى في عصر المصارف التقليدية ذات المقر المحدد مكانياً، وقد كان أقصى ما وصلت إليه من تقدم متمثلاً في إجراء التحويلات المصرفية بإجراءات ورقية معقدة ومقابل رسوم مالية معينة. فإذا كان الركن المادي للسرقة المتمثّل في الاختلاس يمكن أن يطبق على التحويلات المالية غير المشروعة التي تتم عبر المصارف التقليدية فذلك لأن جريمة السرقة من الجرائم ذات القالب الحر لم يحدد المشرّع شكل السلوك الإجرامي لها، يمكن أن يتم بأي فعل يؤدي إلى حرمان المجني عليه من المال المنقول وإدخاله في حيازة الجاني، كذلك الحال بالنسبة لجريمة النصب؛ حيث يتحقق السلوك الإجرامي لها بالاستيلاء على أموال الآخر بالطرق الاحتيالية، فهل ينطبق ذلك على جرائم السرقة والاحتيال التي ترتكب عن طريق التقنية المعلوماتية؟ [1].

وتشمل جرائم السطو على أرقام البطاقات الائتمانية، لعب القمار، التزوير، الجريمة المنظمة، المخدرات، غسيل الأموال، ولعل جرائم هذا القسم أوضح من ناحية معرفة كونها مُجَّرَمة حيث لا تختلف في نتيجتها عن الجرائم التقليدية التي تحمل نفس المسمى والتي يعرف الجميع أنها مخالفة للنظام وللشرع كونهم من الجرائم التي اشتهر محاربتها جنائياً:

(1) عرب، يونس، جرائم الكمبيوتر والانترنت، موسوعة القانون وتقنية المعلومات، منشورات اتحاد المصارف العربية، الطبعة الأولى، الجزء الثاني، 2002م.

المطلب الأوّل

جرائم السطو على أرقام البطاقات الائتمانية

بدأ مفهوم التجارة الإليكترونية ينتشر في السبعينات الميلادية وذلك لسهولة الاتصال بين الطرفين ولإمكانية اختزال العمليات الورقية والبشرية فضلاً عن السرعة في إرسال البيانات وتخفيض تكلفة التشغيل والأهم هو إيجاد أسواق أكثر اتساعاً. ونتيجة لذلك فقد تحول العديد من شركات الأعمال إلى استخدام الانترنت والاستفادة من مزايا التجارة الإليكترونية، كما نحول تبعاً لذلك الخطر الذي كان يهدد التجارة السابقة ليصبح خطراً متوافقاً مع التجارة الإليكترونية. فالاستيلاء على بطاقات الائتمان عبر الانترنت أمر ليس بالصعوبة بمكان إطلاقاً، فـ «لصوص بطاقات الائتمان مثلاً يستطيعون الآن سرقة مئات الألوف من أرقام البطاقات في يوم واحد من خلال شبكة الانترنت، ومن ثم بيع هذه المعلومات للآخرين» [1]. وقد وقعت بالفعل عدة حوادث ومن ذلك حادثة شخص ألماني قام بالدخول غير المشروع إلى أحد مزود الخدمات، واستولى على أرقام بطاقات ائتمانية الخاصة بالمشتركين ومن ثم هدد مزود الخدمة بإفشاء أرقام تلك البطاقات ما لم يستلم فدية وقد تمكنت الشرطة الألمانية من القبض عليه. كما قام شخصان في عام (1994م) بإنشاء موقع على الانترنت مخصص لشراء طلبات يتم بعثها فور تسديد قيمتها إليكترونياً، ولم تكن الطلبات لتصل إطلاقاً حيث كان الموقع وهمي قصد منه النصب والاحتيال وقد قبض على مؤسسيه لاحقاً[2]، وأثبت

---

(1) الخليل، عماد علي، التكييف القانوني لإساءة استخدام أرقام البطاقات عبر شبكة الانترنت، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، الذي نظمته كلية الشريعة والقانون، بجامعة الإمارات العربية المتحدة، عام2000م.

(2) عرب، يونس، جرائم الكمبيوتر والانترنت، موسوعة القانون وتقنية المعلومات، المرجع السابق.

شبكة (MSNBC) عملياً سهولة الحصول على أرقام بطاقات الائتمان من الانترنت؛ حيث قامت بعرض قوائم تحتوي على أكثر من (2500) رقم بطاقة ائتمان حصلت عليها من سبعة مواقع للتجارة الإليكترونية باستخدام قواعد بيانات متوفرة تجارياً، ولم يكن يصعب على أي متطفل استخدام ذات الوسيلة البدائية للاستيلاء على أرقام تلك البطاقات واستخدامها في عمليات شراء يدفع قيمتها أصحابها الحقيقين. ويقترح بعض الخبراء باستخدام بطاقة ائتمان خاصة بالانترنت يكون حدها الائتماني معقول بحيث يُقلل من مخاطر فقدانها والاستيلاء غير المشروع عليها، وهو الأمر الذي بدأت بعض البنوك الدولية والمحلية في تطبيقه أخيراً [1]. ويتعدى الأمر المخاطر الأمنية التي تتعرَّض لها بطاقات الائتمان فنحن في بداية ثورة نقدية تعرف باسم النقود الإليكترونية (Electronic Cach) أو (Cyber Cash) والتي يتنبأ لها أن تكون مكملة للنقود الورقية والبلاستيكية (بطاقات الائتمان)، وأن يزداد الاعتماد عليها والثقة بها، كما أن هناك الأسهم والسندات الإليكترونية المعمول بها في دول الاتحاد الأوروبي والتي أقر الكونجرس الأمريكي التعامل بها في عام 1990م، وبالتالي فإن التعامل معها من خلال الانترنت سيواجه مخاطر أمنية ولا شك. ولذلك لجأت بعض الشركات والبنوك إلى العمل سوياً لتجاوز هذه المخاطر كالاتفاق الذي وقع بين مؤسسة هونج كونج وشنغهاي البنكية (HSBC) وهي من أكبر المؤسسات المصرفية في هونج كونج وشركة كومباك للحاسب الآلي وذلك لتطوير أول نظام إلى آمن للتجارة الإليكترونية والذي يمنح التجار خدمة نظام دفع أمن لتمرير عمليات الشراء عبر الانترنت [2].
وجرائم السطو على أرقام البطاقات الائتمانية مُجَرَّمة شرعاً وقانوناً؛ حيث تصنف ضمن جرائم السرقات، «فالشارع الإسلامي يرغب في المحافظة

(1) الشافعي، محمد إبراهيم محمد، النقود الإليكترونية، مجلة الأمن والحياة، أكاديمية الشرطة، دبي، س 12، ع1، يناير، 2004م.

(2) الشافعي، محمد إبراهيم محمد، النقود الإليكترونية، مجلة الأمن والحياة، المرجع السابق.

على أموال الناس وصيانتها من كل اعتداء غير مشروع بحيث يُهدد الأمن والاستقرار» (فرحات، 1404هـ: 29). والسرقة من الكبائر المحرمة التي نصت الآيات القرآنية والأحاديث النبوية على تحريمها ووضعت عقوبة رادعة لمرتكبها. قال تعالى: ﴿السَّارِقُ وَالسَّارِقَةُ فَاقْطَعُوا أَيْدِيَهُمَا جَزَاءً بِمَا كَسَبَا نَكَالاً مِنَ اللَّهِ وَاللَّهُ عَزِيزٌ حَكِيمٌ﴾ [1] بل لعن رسول الله السارق نظراً لشناعة فعله وعظيم جرمه، ففي الحديث الذي رواه البخاري في صحيحه عن أبي هريرة رضي الله عنه عن النبي ﷺ قال: « لعن الله السارق، يسرق البيضة فتقطع يده، ويسرق الحبل فتقطع يده». كما نفى الحبيب المصطفى عليه الصلاة والسلام صفة الإيمان عن السارق فروى البخاري في صحيحه عن ابن عباس رضي الله عنهما، عن النبي ﷺ قال: «لا يزني الزاني حين يزني وهو مؤمن، ولا يسرق السارق حين يسرق وهو مؤمن»[2].

ونجد أن **المادة الرابعة** من نظام مكافحة جرائم المعلوماتية السعودي رقم 79 وتاريخ 1428/3/7: يُعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

1 – الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة.

2 – الوصول – دون مسوِّغ نظامي صحيح – إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تُتيحه من خدمات.

وقد تثور هذه المشكلة في حالة الإليكترونية: جهاز لصرف ما

---

(1) سورة المائدة/الآية 38.

(2) صحيح البخاري.

يتجاوز الرصيد الفعلي إذا تم ذلك بواسطة العميل صاحب البطاقة، فالمسألة هنا لا تعدو أن تكون مسألة مديونية بين المؤسسة المالية والعميل ولا يمكن تكييفها بأنها سرقة؛ لأن الاستيلاء على المبلغ لم يتم دون رضاء المؤسسة المالية طالما أن هذه الأخيرة تعلم بأن الجهاز غير مرتبط بسقف حساب العميل حتى لا يتجاوزه.

وجرائم الاستيلاء على النقود الإليكترونية: ويمكن تعريف النقود الإليكترونية بوضوح أكثر بأنها: «قيمة نقدية مخزَّنة على وسيلة إليكترونية مدفوعة مقدماً، وغير مرتبطة بحساب مصرفي، تحظى بقبول غير مَن قام بإصدارها، وتستعمل كأداة دفع». وتتمثَّل أهم عناصرها في أن قيمتها النقدية تشحن على بطاقة بلاستيكية، أو على القرص الصلب للحاسب الشخصي للمستهلك، فهي تختلف عن البطاقات الائتمانية؛ لأن النقود الإليكترونية يتم دفعها مسبقاً، بالإضافة إلى أنها ليست مرتبطة بحساب العميل، فهي أقرب إلى الصكوك السياحية منها إلى بطاقة الائتمان، أي أنها استحقاق عائم على مؤسسة مالية، يتم بين طرفين هما: العميل والتاجر، دون الحاجة إلى تدخل طرف ثالث، كمصدر هذه النقود مثلاً [1]، فهي مجموعة من البروتوكولات والتوقيعات الرقمية التي تتيح للرسالة الإليكترونية أن تحل فعلياً محل تبادل العملات النقدية[2]، ومن هذه البطاقات ما يعمل عن طريق إدخالها إلى المركز الخاص بالمعاملة المصرفية لدى البائع أو الدائن حيث تم انتقال البيانات الاسمية من البطاقة إلى الجهاز الطرفي للبائع تحول عليه نتائج عمليات البيع والشراء إلى البنك الخاص بالبائع [3].

---

(1) الشافعي، محمد إبراهيم محمد، النقود الإليكترونية، مجلة الأمن والحياة، المرجع السابق، يناير، 2004، ص 142-148.

(2) الجنبيهي، منير، والجنبيهي، ممدوح البنوك الإليكترونية ط 2، 2006 م، دار الفكر الجامعي، الإسكندرية، ص47.

(3) بيومي، حجازي عبد الفتاح، صراع الكمبيوتر والانترنت، في القانون العربي النموذجي، المرجع السابق.

المطلب الثاني

القمار عبر الانترنت

كثيراً ما تدخل عملية غسيل الأموال مع أندية القمار المنتشرة، الأمر الذي جعل مواقع الكازينوهات الافتراضية على الانترنت محل اشتباه ومراقبة من قِبل السلطات الأمريكية. وبالرغم من أن سوق القمار في أمريكا يُعتبر الأسرع نمواً على الإطلاق، إلا أن المشكلة القانونية التي تواجه أصحاب مواقع القمار الافتراضية على الانترنت أنها غير مصرَّح لها حتى الآن في أمريكا بعكس نوادي القمار الحقيقية كالمنتشرة في لاس فيجاس وغيرها، ولذلك يلجأ بعض أصحاب تلك المواقع الافتراضية على الانترنت إلى إنشائها وإدارتها من أماكن مجاورة لأمريكا وخاصة في جزيرة انتيجوا على الكاريبي. ويوجد على الانترنت أكثر من ألف موقع للقمار يسمح لمرتاديه من مستخدمي الانترنت ممارسة جميع أنواع القمار التي توفرها المواقع الحقيقية، ومن المتوقَّع أن يُنفق الأمريكيون ما يزيد عن (600) مليار دولار سنوياً في أندية القمار وسيكون نصيب مواقع الانترنت منها حوالي مليار دولار. وقد حاول المشرِّعون الأمريكيون تحريك مشروع قانون يمنع المقامرة عبر الانترنت ويسمح بملاحقة الذين يستخدمون المقامرة السلكية أو الذين يروجون لها سواء كانت هذه المواقع في أمريكا أو خارجها [1]. فإذا كان هذا هو حال القمار ونظرة القوانين الوضعية له، فما هو نظرة الشرع له وهل يوجد في تعاليم الدين الإسلامي ما يُجَرِّم لعب القمار، ويجعله من الأفعال المحرمة شرعاً والمعاقب عليه قانوناً ينظر الإسلام إلى القمار كمحظور شرعي منهي عن فعله ومعاقب على ارتكابه، وقد وردت أدلة متعددة في كتاب الله وفي كتب الأحاديث، أما دليل تحريم القمار من القرآن فهو قوله تعالى: ﴿يَا أَيُّهَا

(1) Laura B. Quarantiello, Tiare Publications, Cyber Crime: How to Protect Yourself from Computer Criminals, 1996.

الَّذِينَ آمَنُوا إِنَّمَا الْخَمْرُ وَالْمَيْسِرُ وَالْأَنصَابُ وَالْأَزْلَامُ رِجْسٌ مِّنْ عَمَلِ الشَّيْطَانِ فَاجْتَنِبُوهُ لَعَلَّكُمْ تُفْلِحُونَ﴾[1] ولم يكتف الشرع بالنهي عن هذا الفعل بل وضّح لأتباعه أن هذا العمل إنما هو من أعمال الشيطان التي يسعى من خلالها إلى إيقاع العداوة والبغضاء بين الناس، ووضح أن في اجتناب هذا الفعل فلاح وصلاح وفوز في الدنيا والآخرة، قال تعالى: ﴿إِنَّمَا يُرِيدُ الشَّيْطَانُ أَنْ يُوقِعَ بَيْنَكُمُ العداوة وَالْبَغْضَاءَ فِي الْخَمْرِ وَالْمَيْسِرِ وَيَصُدَّكُمْ عَنْ ذِكْرِ اللَّهِ وَعَنِ الصَّلَاةِ فَهَلْ أَنْتُمْ مُنْتَهُونَ﴾[2] واتفق المفسرون على أن الميسر هو القمار، فورد توضيح كلمة الميسر في تفسير الجلالين بأنها القمار، أما ابن كثير فقد أورد في تفسيره لهذه الآية، حديثاً رواه أحمد في مسنده عن أبي هريرة رضي الله عنه أن أمير المؤمنين عمر بن الخطاب ﷺ فسَّر الميسر هنا بالقمار، كما ورد تفسير كلمة الميسر أيضاً في فتح القدير بأنها قمار العرب بالأزلام، وكذلك أكد تفسير البغوي بان المراد بالميسر هو القمار، أما البيضاوي فقد وضح أن الميسر سُمي به القمار لأنه أخذ مال الغير بيسر. وفي كتب الحديث ورد ذكر القمار أيضاً فقد ورد في مصنف ابن أبي شيبة عن وكيع قال حدثنا حماد بن نجيح قال: رأيت ابن سيرين مر على غلمان يوم العيد المربد وهم يتقامرون بالجوز، فقال: يا غلمان! لا تقامروا فإن القمار من الميسر، كما أورد في مصنفه أيضاً عن ابن سيرين قال: كل شيء فيه قمار فهو من الميسر، وفيه أيضاً عن عبد الله بن عمرو قال: من لعب بالنرد قماراً كان كآكل لحم الخنزير، ومن لعب بها من غير قمار كان كالمدهن بودك الخنزير. كما أخبر عبد الرزاق في مصنفه عن معمر عن ليث عن مجاهد قال: الميسر القمار كله، حتى الجوز الذي يلعب به الصبيان [3].

وتناولت **المادة السادسة** من نظام مكافحة جرائم المعلوماتية السعودي رقم 79 وتاريخ 1428/3/7:

---

(1) سورة المائدة/الآية 90.

(2) سورة المائدة/الآية 91.

(3) صحيح البخاري.

يُعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

1 - إنتاج ما من شأنه المساس بالنظام العام، أو القيم الدينية، أو الآداب العامة، وحرمة الحياة الخاصة، أو إعداده، أو إرساله، أو تخزينه عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي.

2 - إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، للاتجار في الجنس البشري، أو تسهيل التعامل به.

3 - إنشاء المواد والبيانات المتعلقة بالشبكة الإباحية، أو أنشطة الميسر المخلّة بالآداب العامة، أو نشرها، أو ترويجها.

4 - إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، للاتجار بالمخدرات، أو المؤثرات العقلية، أو ترويجها، أو طرق تعاطيها، أو تسهيل التعامل بها.

المطلب الثالث

تزوير البيانات

تُعتبر من أكثر جرائم نظم المعلومات انتشاراً، فلا تكاد تخلو جريمة من جرائم نظم المعلومات من شكل من أشكال تزوير البيانات، وتتم عملية التزوير بالدخول إلى قاعدة البيانات وتعديل البيانات الموجودة بها أو إضافة معلومات مغلوطة بهدف الاستفادة غير المشروعة من ذلك. وقد وقعت حادثة

في ولاية كاليفورنيا الأمريكية؛ حيث عمدت مدخلة البيانات بنادي السيارات وبناءً لاتفاقية مُسبقة بتغيير ملكية السيارات المسجّلة في الحاسب الآلي بحث تصبح باسم أحد لصوص السيارات، والذي يعمد إلى سرقة السيارة وبيعها وعندما يتقدّم مالك السيارة للإبلاغ يتّضح عدم وجود سجلات للسيارة باسمه وبعد بيع السيارة تقوم تلك الفتاة بإعادة تسجيل السيارة باسم مالكها، وكانت تتقاضي مقابل ذلك مبلغ مائة دولار واستمرت في عملها هذا إلى أن قبض عليها، وفي الحادثة الأخرى قام مشرف تشغيل الحاسب بأحد البنوك الأمريكية بعملية تزوير حسابات أصدقائه في البنك بحيث تزيد أرصدتهم ومن ثم يتم سحب تلك المبالغ من قِبل أصدقائه، وقد نجح في ذلك وكان ينوي التوقف قبل موعد المراجعة الدورية لحسابات البنك، إلا أن طمع أصدقاءه أجبره على الاستمرار إلى أن قبض عليه [1]. ومما لا شك فيه أن البدء التدريجي في التحول إلى الحكومات الإليكترونية سيزيد من فرص ارتكاب مثل هذه الجرائم حيث سترتبط الكثير من الشركات والبنوك بالانترنت مما يسهل الدخول على تلك الأنظمة من قِبل محترفي اختراق الأنظمة، وتزوير البيانات لخدمة أهدافهم الإجرامية. وجرائم التزوير ليست بالجرائم الحديثة، ولذا فإنه لا تخلو الأنظمة من قوانيين واضحة لمكافحتها والتعامل معها جنائياً وقضائياً، و«تكفي التشريعات الحالية لتجريمها وتحديد العقوبة عليها» [2]. وعالجت أنظمة المملكة العربية السعودية جرائم التزوير بشكل مفصّل حيث صدر المرسوم الملكي رقم (114) وتاريخ 1380/11/26هـ بالمصادقة على نظام مكافحة التزوير، ومن ثم تم التعديل على هذا النظام ليواكب المستجدات، وذلك بالمرسوم الملكي رقم (53) وتاريخ 1382/11/5هـ، كما صدر نظام جزائي خاص بتزوير وتقليد النقود وذلك بالمرسوم الملكي رقم

---

(1) Tom forester, Essential proplems to Hig-Tech Society First MIT Pres edition, Cambridge, Massachusetts, 1989, p 104.

(2) ياسين، صباغ محمد محمد، الجهود الدولية والتشريعية لمكافحة الإرهاب وقرب العالم الجديد، دار الرضوان، القاهرة، 2005م.

(12) وتاريخ 1379/7/20هـ [1] بالإضافة إلى العقوبات الواردة في نظام مكافحة جرائم المعلوماتية السعودي رقم 79 الصادر بتاريخ 1428/3/7 في **المادة الرابعة:** يُعاقب بالسجن مدة لا تزيد على ثلاث سنوات، وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

1 - الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة.

2 - الوصول - دون مسوّغ نظامي صحيح - إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تُتيحه من خدمات

وإن كان كل موظف يضع أثناء ممارسة مهامه وثيقة مزورة في كليتها، أو جزء منها، أو زور وثيقة صحيحة، ما يهمنا في هذا الصدد محل جريمة التزوير لأن هذه الأخيرة من الجرائم ذات القالب الحر التي لم يُحدد المشرِّع فيها شكلاً معنياً للسلوك الإجرامي فيه؛ لكنه حدَّد محل هذا السلوك بالوثيقة دون أن يعرفها، أو يُحدد مضمونها تاركاً للفقه والقضاء هذه المهمة[2].

فالوثيقة هي مجموعة من المعاملات والرموز التي تُعبر تعبيراً اصطلاحياً عن مجموعة مترابطة من الأفكار والمعاني الصادرة عن شخص أو أشخاص معينين، وتكمن القيمة الحقيقية لها ليس في مادتها أو ما تحتويه، بل تكمن فيما لهذا التعبير من دلالة اجتماعية [3].

---

(1) موقع السوق الخليجي، 1423هـ.

(2) حسين، محمد عبد الظاهر، المسئولية القانونية في مجال شبكات الانترنت، دار النهضة العربية، القاهرة 2002م.

(3) حسني، محمود نجيب، شرح قانون العقوبات، القسم الخاص، الجرائم المضرة بالمصلحة العامة، دار النهضة العربية، القاهرة 1972م.

فجوهر جريمة التزوير هو الإخلال بالثقة العامة التي أراد المشرّع حمايتها في هذه الوثيقة لما لها من آثار قانونية باعتبارها وسيلة للإثبات[1].

ولما كان ذلك، فإن قوة الوثيقة في الإثبات هي جوهر الحماية الجنائية لها، ومن هنا ذهبت بعض الآراء الفقهية إلى أن كل مادة تصلح للإثبات يجوز أن تكون محلاً للتزوير مهما كان شكلها، أو مساحتها ولا أهمية للمادة المستعمَلة في الكتابة يستوي أن تكون مصنوعة من خشب أو جلد [2]، فإذا كانت فكرة التوسُّع في مفهوم الوثيقة مطروحة في الفقه الجنائي قبل ظهور جرائم المعلوماتية، فإن هذا التوسُّع يبدو أكثر إلحاحاً في ظل الفراغ التشريعي لمواجهة جرائم التزوير المرتكبة بواسطة الحاسب الآلي، إلا أن هذا الاتجاه واجه نقداً شديداً؛ حيث ذهب جانب من الفقه الفرنسي قبل صدور القانون رقم 19 لسنة 1988 م الخاص بالغش المعلوماتي إلى رفض اعتبار التعبير الواقع على الاسطوانات الممغنطة تزويراً، استناداً إلى اعتبارين أولهما انتفاء الكتابة؛ لأن التغيير انصبّ على نبضات إليكترومغناطيسية، والثاني هو عدم التيقُّن من صلاحيتها في الإثبات [3]. يؤيد هذا الرأي قياس ذلك على انتفاء التزوير في التغيير الذي يطرأ على الصوت المسجل، والعلة هي انعدام عنصر الكتابة، بالإضافة إلى أن النبضات الإليكترومغناطيسية تُمثل جزءً من ذاكرة الآلة أو برنامج تشغيلها وهو ما يمكن أن يتحقق معه الإتلاف أو التقليد إذا توافرت شروطهما، وقد بدأ الفكر القانوني الحديث يقبل فكرة الوثيقة الإليكترونية استناداً إلى أن المادة التي تصنع منها الوثيقة ليست عنصراً فيها[4].

---

(1) الشوا، محمد سامي، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة 1994م.

(2) المرصفاوي، حسن صادق، قانون العقوبات الخاص، منشأة المعارف، الإسكندرية، مصر 1991م.

(3) الشوا، محمد سامي، ثورة المعلومات وانعكاساتها على قانون العقوبات، المرجع السابق ص 155

(4) حسين، محمد عبد الظاهر، المسئولية القانونية في مجال شبكات الانترنت، المرجع السابق

أن مجاراة التقديم العلمي والتكنولوجي تتطلب تجاوز المفهوم التقليدي للوثيقة أو حصره في الورق المكتوب. ويمكن لنا في هذه الحالة أن نجد سنداً لهذه الفكرة ومنطلقاً لها أن المشرِّع المدني في الأصل رغم أخذه بمبدأ سيادة الدليل الكتابي على غيره من طرق الإثبات، إلا أنه أورد عليه بعض الاستثناءات فقبل الإثبات بالبينة فيما كان يجب إثباتها كتابة في حالات حددتها المواد 387 289 391 من القانون المدني الليبي، وهي اتفاق الأطراف على الإثبات بالبينة، أو وجود مانع يحول دون الحصول على الدليل الكتابي فإذا اتفق الأطراف على الإثبات بالبينة يكون على القاضي أن يعتد بها استناداً إلى عدم تعلق القواعد الموضوعية في الإثبات بالنظام العام، مما يمكن القول معه على إمكانية اتفاق الأطراف على الإثبات بالوسائل الإليكترونية وهو ما يعد بداية لعصر الوثائق الإليكترونية [1].

المطلب الرابع

الجرائم المنظمة عبر الانترنت

يتبادر إلى الذهن فور التحدث عن الجريمة المنظمة عصابات المافيا كون تلك العصابات من أشهر المؤسسات الإجرامية المنظمة والتي بادرت بالأخذ بوسائل التقنية الحديثة سواء في تنظيم أو تنفيذ أعمالها، ومن ذلك إنشاء مواقع خاصة بها على شبكة الانترنت لمساعدتها في إدارة العمليات، وتلقّي المراسلات، واصطياد الضحايا، وتوسيع أعمال، وغسيل الأموال، كما تستخدم تلك المواقع في إنشاء مواقع افتراضية تُساعد المنظمة في تجاوز قوانين بلد محدَّد بحيث تعمل في بلد آخر يسمح بتلك الأنشطة. ويوجد على

(1) عبادة، عبادة أحمد، التدمير المتعمد لأنظمة المعلومات الإليكترونية مركز البحوث والدراسات، شرطة دبي بدولة الإمارات العربية المتحدة 2005 م

الشبكة (210) موقع يحتوي اسم نطاقها على كلمة مافيا، في حين يوجد (24) موقعاً يحتوي على كلمة مافيا، كما وجد (4) مواقع للمافيا اليهودية. وقد خصص بعض هذه المواقع للأعضاء فقط، ولم يسمح لغيرهم بتصفُّح تلك المواقع في حين سمحت بعض المواقع للعامة بتصفُّح الموقع، وقامت مواقع أخرى بوضع استمارة تسجيل لمن يرغب في الانضمام إلى العصابة من الأعضاء الجدد[1]، والجريمة المنظمة ليست وليدة التقدم التقني وإن كانت استفادت كثيراً منه، فـ «الجريمة المنظمة وبسبب تقدم وسائل الاتصال والتكنولوجيا والعولمة أصبحت غير محدَّدة لا بقيود الزمان ولا بقيود المكان وإن ما أصبح انتشارها على نطاق واسع وكبير وأصبحت لا تحدها الحدود الجغرافية» [2]، كما استغلت عصابات الجريمة المنظمة «الإمكانيات المتاحة في وسائل الانترنت في تخطيط وتمرير وتوجيه المخططات الإجرامية وتنفيذ وتوجيه العمليات الإجرامية بيسر وسهولة»[3] وهناك مَن يرى أن الجريمة المنظمة والإرهاب هما وجهان لعملة واحدة، فأوجه التشابه بينهما كبير حيث يسعى كلاهما إلى إفشاء الرعب والخوف، كما أنهما يتفقان في أسلوب العمل والتنظيم وقد يكون أعضاء المنظمات الإرهابية هم أساساً من محترفي الجرائم المنظمة؛ حيث يسعون للاستفادة من خبراتهم الإجرامية في التخطيط والتنفيذ، فهناك صلة وتعاون وثيق بينهما [4] وحظيت مكافحة الجريمة المنظمة باهتمام دولي بدأ

---

(1) حسين، محمد عبد الطاهر، المسئولية القانونية في مجال شبكات الانترنت، المرجع السابق

(2) علي، عبد الصبور عبد القوي، الجريمة الإليكترونية، دار العلوم للنشر والتوزيع، القاهرة 2007م.

(3) عفيفي، عفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، 2003.

(4) سقر، حسن بن محمد، الإرهاب والعنف في ميزان الشريعة الإسلامية والقانون الدولي، بحث مقدم لمجمع الفقه الإسلامي الدولي، الدورة الرابعة عشرة، الدوحة، قطر 2003/1/11م.

بمؤتمر الأمم المتحدة السابع عام (1985م) لمنع الجريمة حيث اعتمد خطة عمل ميلانو والتي أوصت بعدة توصيات حيال التعامل مع الجريمة المنظمة والقضاء عليها. وتبع ذلك الاجتماع الإقليمي التحضيري عام (1988م) الذي أقر فيه المبادئ التوجيهية لمنع الجريمة المنظمة ومكافحتها، ثم المؤتمر الثامن لمنع الجريمة بفنزويلا عام (1990م)، فالمؤتمر الوزاري العالمي المعني بالجريمة المنظمة عبر الوطنية في نابولي بإيطاليا عام (1994م) والذي عبّر عن إرادة المجتمع الدولي بتعزيز التعاون الدولي وإعطاء أولوية عليا لمكافحة الجريمة المنظمة. كما وضعت لجنة مكافحة الجرائم المنظمة مقترحات للعمل العربي في مكافحة الإرهاب والتي وافق عليها مجلس وزراء الداخلية العرب في دورته السادسة، وفي عام (1996م) وافق المجلس في دورته الثالثة عشر على مدونة سلوك طوعية لمكافحة الإرهاب، ووافق في عام (1997م) وفي الدورة الرابعة عشر على استراتيجية عربية لمكافحة الإرهاب وفي عام (1998م) تم إقرار الاتفاقية العربية لمكافحة الإرهاب من قبل مجلس وزراء الداخلية والعدل العرب [1]

وتناول نظام مكافحة جرائم المعلوماتية السعودي رقم 79 الصادر بتاريخ 1428/3/7 في المادة السابعة: يُعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

1 - إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها أو ترويج أفكارها أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أداة تستخدم في الأعمال الإرهابية.

---

(1) سفر، حسن بن محمد، الإرهاب والعنف في ميزان الشريعة الإسلامية والقانون الدولي، المرجع السابق.

2 - الدخول غير المشروع إلى موقع إليكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني.

المطلب الخامس

الاتجار بالمخدرات عبر الانترنت

كثيراً ما يُحذّر أولياء الأمور أبنائهم من رفقاء السوء خشية من تأثيرهم السلبي عليهم وخاصة في تعريفهم على المخدرات، فالصاحب ساحب كما يقول المثل وهذا صحيح ولا غبار عليه، ولكن وفي عصر الانترنت أُضيف إلى أولياء الأمور مخاوف جديدة لا تقتصر على رفقاء السوء فقط بل يمكن أن يُضاف إليها مواقع السوء - إن صح التعبير - ومن تلك المواقع طبعاً المواقع المنتشرة في الانترنت والتي لا تتعلق بالترويج للمخدرات وتشويق النشأ لاستخدامها بل تتعداه إلى تعليم كيفية زراعة وصناعة المخدرات بكافة أصنافها وأنواعها وبأبسط الوسائل المتاحة. والأمر هنا لا يحتاج إلى رفاق سوء بل يمكن للمراهق الانزواء في غرفته والدخول إلى أي من هذه المواقع ومن ثم تطبيق ما يقرأه ويؤكد هذه المخاوف أحد الخبراء التربويين في بتسبيرج بالولايات المتحدة والذي أكّد أن ثمة علاقة يمكن ملاحظتها بين ثالوث المراهقة والمخدرات والانترنت. ولا تقتصر ثقافة المخدرات على تلك المواقع فقط بل تُساهم المنتديات وغرف الدردشة في ذلك أيضاً [1]. وبالرغم من انتشار المواقع الخاصة بالترويج للمخدرات وتعليم كيفية صنعها إلا أن

---

(1) رستم، هشام محمد فريد، جرائم الحاسوب كصورة من صور الجرائم الاقتصادية المستحدثة، مجلة الدراسات القانونية، جامعة أسيوط، العدد 17 - 1995م.

هذه المواقع لم تدق جرس الإنذار بعد ولم يهتم بآثارها السلبية وخاصة على النشأ كما فعلته المواقع الإباحية وخاصة في الدول التي تعرف باسم الدول المتقدمة. وقد اعترف الناطق الرسمي للتحالف المناهض للمخدرات بأنهم خسروا الجولة الأولى في ساحة الانترنت حيث لم يطلق موقعهم الخاص على الشبكة http://www.cadca.org إلا منذ عامين فقط[1]، واهتمت دول العالم قاطبة بمكافحة جرائم المخدرات، وعقدت المؤتمرات، والاتفاقيات الدولية المختلفة، ومنها الاتفاقية الوحيدة لمكافحة المخدرات عام (1961م)، اتفاقية المؤثرات العقلية عام (1971م)، واتفاقية الأمم المتحدة لمكافحة الاتجار غير المشروع في المخدرات والمؤثرات العقلية عام (1988م). وعلى المستوى العربي تم عام (1996م) إقرار الاتفاقية العربية لمكافحة الاتجار غير المشروع في المخدرات والمؤثرات العقلية، كما تم عام (1986م) إقرار القانون العربي النموذجي الموحد للمخدرات. أما على المستوى المحلي فقد صدر نظام مكافحة الاتجار بالمواد المخدرة في المملكة العربية السعودية بقرار مجلس الوزراء رقم (11) عام (1374هـ) وألحق به قرار هيئة كبار العلماء رقم (138) وتاريخ 1407/6/20هـ الخاص بإعدام مهربي المخدرات أو مَن يقبض عليه في قضية ترويج للمرة الثانية، والموافق عليه بالأمر السامي رقم (4/ب/966) وتاريخ 1407/7/10هـ.

ولم يهمل المنظِّم السعودي النص على تلك الجريمة في المادة السادسة الفقرة 4 من نظام مكافحة جرائم المعلوماتية السعودي رقم 79 الصادر بتاريخ 1428/3/7:

يُعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

---

(1) القدهي، مشعل عبدالله. (1422هـ). المواقع الإباحية على شبكة الانترنت وأثرها على الفرد والمجتمع. (1422/7/29هـ) //http://www. minshawi. com/gadhi. htm

1 – إنتاج ما من شأنه المساس بالنظام العام، أو القيم الدينية، أو الآداب العامة، وحرمة الحياة الخاصة، أو إعداده، أو إرساله، أو تخزينه عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي.

2 – إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، للاتجار في الجنس البشري، أو تسهيل التعامل به.

3 – إنشاء المواد والبيانات المتعلقة بالشبكة الإباحية، أو أنشطة الميسر المخلّة بالآداب العامة أو نشرها أو ترويجها.

4 – إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، للإتجار بالمخدرات، أو المؤثرات العقلية، أو ترويجها، أو طرق تعاطيها، أو تسهيل التعامل بها.

المطلب السادس

غسيل الأموال

مصطلح غسيل الأموال مصطلح حديث نسبياً ولم يكن معروفاً لرجال الشرطة فضلاً عن العامة، وقد بدأ استخدام المصطلح في أمريكا نسبة إلى مؤسسات الغسيل التي تملكها المافيا، وكان أول استعمال قانوني لها في عام (1931م) إثر محاكمة لأحد زعماء المافيا تمت في أمريكا، واشتملت مصادرة أموال قيل أنها متأتية من الاتجار غير المشروع بالمخدرات. واختلف الكثير في تعريف غسيل الأموال وقد يكون التعريف الشامل هو: «أي عملية من شأنها إخفاء المصدر غير المشروع الذي اكتسبت منه الأموال»، ومن البديهي أن يأخذ

المجرمون بأحدث ما توصّلت إليه التقنية لخدمة أنشطتهم الإجرامية، ويشمل ذلك بالطبع طرق غسيل الأموال التي استفادت من عصر التقنية فلجأت إلى الانترنت لتوسعة وتسريع أعمالها في غسيل أموالها غير المشروعة، ويجد المتصفّح للانترنت مواقع متعددة تتحدث عن غسيل أموال كما يجد ولا شك أيضاً المواقع التي تستخدم كساتر لعمليات غسيل الأموال ومنها المواقع الافتراضية لنوادي القمار، والتي قام مكتب المباحث الفيدرالية (FBI) الأمريكي بمراقبة بعض هذه المواقع واتضح أنها تتواجد في كاراكاو، جزر الانتيل، جزيرة أنتيجوا وجمهورية الدومينكان، وقد أسفرت التحريات التي استمرت خمسة أشهر عن اعتقالات واتهامات للعديد من مدراء تلك المواقع.
ومن المميزات التي يعطيها الانترنت لعملية غسيل الأموال السرعة، إغفال التوقيع وأن إعدام الحواجز الحدودية بين الدول، كما تُساهم البطاقات الذكية، والتي تُشبه في عملها بطاقات البنوك المستخدمة في مكائن الصرف الآلية، في تحويل الأموال بواسطة المودم أو الانترنت مع ضمان تشفير وتأمين العملية.
كل هذا جعل عمليات غسيل الأموال عبر الانترنت تتم بسرعة أكبر وبدون ترك أي آثار في الغالب. ويقدر المتخصصون المبالغ التي يتم تنظيفها سنوياً بحوالي (400) مليار دولار [1]. وإلى عهد قريب لم تكن جرائم غسيل أموال تُشكل جرماً بذاتها إلى أن تضخّمت الأموال المتحصلة من الجرائم وخاصة من تجارة المخدرات فأصدرت بعض الدول قوانين خاصة تسمح بتعقّب وتجميد ومصادرة عائدات الجرائم الخطرة، فأصدرت الولايات المتحدة الأمريكية عام (1970م) قانون المنظمات القائمة على الابتزاز والنساء، وقانون منع ومكافحة جرائم إساءة استخدام العقاقير المخدرة، كما أصدرت مصر عام (1971م) القانون رقم (34) والخاص بتنظيم فرض الحراسة على الأموال المكتسبة بطرق غير مشروعة، كما أقر القانون العربي النموذجي الموحّد للمخدرات الصادر عن مجلس وزراء الداخلية العرب عام (1986م) مكافحة

---

(1) محمد، عادل ريان، (1995م)، جرائم الحاسب الآلي وأمن البيانات، العربي، (440)، 73 - 77.

جرائم غسيل الأموال وخاصة في مادته التاسعة والأربعين والتي سمحت للمحكمة المختصة بحجز الأموال المتحصلة من تجارة المخدرات والتحقق من مصادر تلك الأموال. كما أصدرت بريطانيا وآيرلندا عام (1986م) قانون يسمح بمصادرة عائدات الجريمة. وأصدرت استراليا عام (1987م) قانوناً يسمح بمصادرة أموال الشخص المدان في جرائم اتحادية. ولم تتخلَّف المملكة العربية السعودية عن ركب محاربة جرائم غسيل الأموال فقد كانت المملكة من ضمن دول العالم الـ (106) اللذين وقعوا عام (1988م) على اتفاقية الأمم المتحدة لمكافحة الاتجار غير المشروع في المخدرات والمؤثرات العقلية والتي كانت أول خطوة دولية مهمة لتعريف غسيل الأموال وتحديد الأفعال الواجب تجريمها[1].

تناول نظام مكافحة جرائم المعلوماتية السعودي رقم 79 الصادر بتاريخ 7/ 3/1428 هـ النص على عقوبة تلك الجريمة في المادة السادسة:

يُعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

1 - إنتاج ما من شأنه المساس بالنظام العام، أو القيم الدينية، أو الآداب العامة، وحرمة الحياة الخاصة، أو إعداده، أو إرساله، أو تخزينه عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي.

2 - إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، للاتجار في الجنس البشري، أو تسهيل التعامل به.

---

(1) مندورة، محمد محمود، الجرائم الحاسب الآلية، دورة فيروس الحاسب الآلي، مكتب الأفاق المتحدة: الرياض، 1410هـ.

3 - إنشاء المواد والبيانات المتعلقة بالشبكة الإباحية، أو أنشطة الميسر المخلَّة بالآداب العامة أو نشرها أو ترويجها.

4 - إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، للاتجار بالمخدرات، أو المؤثرات العقلية، أو ترويجها، أو طرق تعاطيها، أو تسهيل التعامل بها.

المبحث الثالث

جرائم القرصنة

يُقصد بجرائم القرصنة هنا الاستخدام أو النسخ غير المشروع لنظم التشغيل أو لبرامج الحاسب الآلي المختلفة. وقد تطورت وسائل القرصنة مع تطور التقنية، ففي عصر الانترنت تطورت صور القرصنة واتسعت وأصبح من الشائع جداً العثور على مواقع بالانترنت خاصة لترويج البرامج المقرصنة مجاناً أو بمقابل مادي رمزي. وأدّت قرصنة البرامج إلى خسائر مادية ناهضة جداً وصلت في العام (1988م) إلى (11) مليار دولار أمريكي في مجال البرمجيات وحدها، ولذلك سعت الشركات المختصة في صناعة البرامج إلى الاتحاد وإنشاء منظمة خاصة لمراقبة وتحليل سوق البرمجيات ومن ذلك منظمة اتحاد برمجيات الأعمال أو ما تُعرف اختصاراً بـ (BSA)، والتي أجرت دراسة تبين منها أن القرصنة على الانترنت ستطغى على أنواع القرصنة الأخرى، ودق هذا التقرير ناقوس الخطر للشركات المعنية فبدأت في طرح الحلول المختلفة لتفادي القرصنة على الانترنت، ومنها تهديد بعض الشركات بفحص القرص الصلب لمتصفحي مواقعهم على الانترنت لمعرفة مدى استخدام المتصفح للموقع لبرامج مقرصنة إلا أن تلك الشركات تراجعت عن هذا التهديد إثر محاربته من قِبل جمعيات حماية الخصوصية لمستخدمي الانترنت. كما قامت بعض تلك الشركات بالاتفاق مع مزودي الخدمة لإبلاغهم عن أي مواقع مخصصة للبرامج المقرصنة تنشأ لديهم وذلك لتقديم شكوى ضدهم ومقاضاتهم أن أمكن أو إقفال تلك المواقع على أقل تقدير والقرصنة عربياً لا تختلف كثيراً عن القرصنة عالمياً إن لم تسبقها بخطوات خاصة في ظل عدم توفر حقوق الحماية الفكرية أو في عدم جدية تطبيق هذه القوانين إن وجدت[1] وقوانين حماية الملكية تُعتبر من الأنظمة الحديثة في الدول العربية؛ حيث بدأت الفكرة

---

(1) مندورة، محمد محمود، الجرائم الحاسب الآلية، دورة فيروس الحاسب الآلي، المرجع السابق.

من الدول الرأسمالية ومن ثم بدأت الدول الأخرى تطبيقها وإدراجها في أنظمتها، وقد اهتمت دول الخليج بحماية الملكية الفكرية أيضاً فقامت أمانة مجلس التعاون الخليجي وفي الاجتماع الثاني للوزراء المسئولين عن الثقافة المنعقد بالرياض في 1987/9/15م بوضع لائحة استرشادية للنظام الموحَّد لحماية حقوق المؤلف في دول المجلس. ولم يكن هذا هو آخر المشوار بل البداية حيث توالت دول الخليج في إصدار قوانين الحماية الفكرية، ففي سلطنة عمان مثلاً صدر قانون الملكية الفكرية بالمرسوم السلطاني رقم (97/65) وتاريخ 1418/5/3هـ وفي الكويت صدر القانون رقم (64) لعام (1999م) بشأن حقوق الملكية الفكرية. أما المملكة العربية السعودية فكانت سبّاقة إلى إصدار تنظيمات خاصة لمحاربة القرصنة فصدر قرار مجلس الوزراء رقم (56) وتاريخ 1409/4/14هـ بالموافقة على نظام براءات الاختراع، ثم صدر قرار مجلس الوزراء رقم (30) وتاريخ 1410/2/25هـ بالموافقة على نظام حماية حقوق المؤلف. ووافق مجلس الوزراء الموقر في جلسته بتاريخ 1420/6/17هـ على تشكيل اللجنة الدائمة لحقوق الملكية الفكرية من ممثلين عن وزارات التجارة، الإعلام، الداخلية، الخارجية، العدل، الصناعة والكهرباء، البترول والثروة المعدنية، المالية والاقتصاد الوطني (مصلحة الجمارك)، ديوان المظالم، ومدينة الملك عبد العزيز للعلوم والتقنية، ويكون مقرها ورئاستها بوزارة التجارة، وحددت مهام اللجنة بمتابعة ودراسة ما يستجد من أمور في مجال حقوق الملكية الفكرية، وإعداد التوصيات اللازمة بما يتناسب مع متطلبات الاتفاقيات الدولية ذات العلاقة، وفي مقدمتها اتفاقية الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية [1].

وتناول نظام مكافحة جرائم المعلوماتية السعودي رقم 79 الصادر بتاريخ 1428/3/7 هـ النص على عقوبة تلك الجريمة في المادة الثالثة فقرة 2و3:

يُعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم

(1) موقع وزارة التجارة والصناعة السعودية.

المعلوماتية الآتية:

1 - ....

2 - الدخول غير المشروع لتهديد شخص أو ابتزازه؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً.

3 - الدخول غير المشروع إلى موقع إليكتروني، أو الدخول إلى موقع إليكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه.

4 - ....

المبحث الرابع

التجسُّس الإليكتروني

في عصر المعلومات وبفعل وجود تقنيات عالية إلى الطرق حدود الدولة مستباحة بأقمار التجسُّس والبث الفضائي» [1]، والعالم العربي والإسلامي كان ولا يزال مستهدف أمنياً وثقافياً وفكرياً وعقدياً لأسباب لاتخفى على أحد. وقد تحولت وسائل التجسُّس من الطرق التقليدية إلى الطرق الإليكترونية خاصة مع استخدام الانترنت وانتشاره عربياً وعالمياً. ولا تكمن الخطورة في استخدام الانترنت ولكن في ضعف الوسائل الأمنية المستخدمة في حماية الشبكات الخاصة بالمؤسسات والهيئات الحكومية ولا يمكن حتماً الاعتماد على وسائل الحماية التي تنتجها الشركات الأجنبية فهي ليست في مأمن ولا يمكن الاطمئنان لها تماماً ولا يقتصر الخطر على محاولة اختراق الشبكات والمواقع على العابثين من مخترقي الأنظمة أو ما يعرفون اصطلاحاً (hackers) فمخاطر هؤلاء محدودة وتقتصر غالباً على العبث أو إتلاف المحتويات والتي يمكن التغلب عليها باستعادة نسخة أخرى مخزنة في موقع أمن، أما الخطر الحقيقي فيكمن في عمليات التجسُّس التي تقوم بها الأجهزة الاستخباراتية للحصول على أسرار ومعلومات الدولة ومن ثم إفشائها لدول أخرى تكون عادة معادية، أو استغلالها بما يضر بالمصلحة الوطنية للدولة. وقد وجدت بعض حالات التجسُّس الدولي ومنها ما اكتشف أخيراً عن مفتاح وكالة الأمن القومي الأمريكية (NSA) والتي قامت براعته في نظام التشغيل الشهير وندوز، وربما يكون هذا هو أحد الأسباب الرئيسية التي دعت الحكومة الألمانية بإعلانها في الآونة الأخيرة عن استبدالها لنظام التشغيل وندوز بأنظمة أخرى. كما كشف أخيراً النقاب عن شبكة دولية ضخمة للتجسُّس الإليكتروني تعمل تحت إشراف وكالة الأمن القومية الأمريكية بالتعاون مع أجهزة الاستخبارات والتجسس في كندا، بريطانيا، استراليا ونيوزيلندا ويطلق عليها اسم (-ECH

---

(1) راجع الرابط zhektmenkom.maktoobblog.com

ELON) لرصد المكالمات الهاتفية والرسائل بكافة أنواعها سواء ما كان منها برقياً، تلكسياً، فاكسياً أو إليكترونياً[1]. وخصص هذا النظام للتعامل مع الأهداف غير العسكرية وبطريقة تجعله يفترض كميات هائلة جداً من الاتصالات والرسائل الإليكترونية عشوائياً باستخدام خاصية الكلمة المفتاح بواسطة الحاسبات المتعددة والتي تم إنشاء العديد من المحطات السرية حول العالم للمساهمة في مراقبة شبكات الاتصالات الدولية ومنها محطة رصد الأقمار الصناعية الواقعة في منطقة وأي هوباي بجنوب نيوزيلندا، ومحطة جير الدتون الموجودة باستراليا، والمحطة الموجودة في منطقة موروينستو في مقاطعة كورنوول ببريطانيا، والمحطة الواقعة في الولايات المتحدة الأمريكية بمنطقة شوجرجروف وتبعد (250) كيلومترا جنوب واشنطن دي سي، وأيضاً المحطة الموجودة بولاية واشنطن على بعد (200) كيلومتر جنوب غرب مدينة سياتل. ولا يقتصر الرصد على المحطات الموجهة إلى الأقمار الصناعية والشبكات الدولية الخاصة بالاتصالات الدولية [2]، بل يشمل رصد الاتصالات التي تجرى عبر أنظمة الاتصالات الأرضية وكذا الشبكات الإلكترونية. أي أنه يرصد جميع الاتصالات التي تتم بأي وسيلة. ويعتبر الأفراد والمنظمات والحكومات اللذين لا يستخدمون أنظمة الشفرة التأمينية أو أنظمة كودية لحماية شبكاتهم وأجهزتهم، أهدافاً سهلة لشبكة التجسّس هذه، وإن كان هذا لا يعني بالضرورة أن الأهداف الأخرى التي تستخدم أنظمة الشفرة في مأمن تام من الغزوات الاستخباراتية لهذه الشبكة ومثيلاتها، ولا يقتصر التجسّس على المعلومات العسكرية أو السياسية بل تعداه إلى المعلومات التجارية والاقتصادية بل وحتى الثقافية [3] فمع توسع التجارة الإليكترونية عبر شبكة الانترنت تحولت الكثير من مصادر المعلومات إلى أهداف للتجسّس التجاري

---

(1) David J. David, Internet Detective-An Investigator's Guide, Police Research Group, 1998.

(2) Interpol, Scoping and responding to information Technology crime in Asia-South Pacific Region, 2001.

(3) Eoghan Casey, Digital Evidence and Computer Crime, Academic Press,. 1 st edition, 2000.

ففي تقرير صدر عن وزارة التجارة والصناعة البريطانية أشار إلى زيادة نسبة التجسُّس على الشركات من (36%) عام (1994م) إلى (45%) عام (1999م)، كما أظهر استفتاء أجرى عام (1996م) لمسئولي الأمن الصناعي في الشركات الأمريكية حصول الكثير من الدول وبشكل غير مشرّع على معلومات سرية لأنشطة تجارية وصناعية في الولايات المتحدة الأمريكية [1]. ومن الأساليب الحديثة للتجسس الإليكتروني أسلوب إخفاء المعلومات داخل المعلومات وهو أسلوب شائع وإن كان ليس بالأمر السهل، ويتلخّص هذا الأسلوب في لجوء المجرم إلى إخفاء المعلومة الحساسة المستهدفة بداخل معلومات أخرى عادية داخل الحاسب الآلي ومن ثم يجد وسيلة ما لتهريب تلك المعلومة العادية في مظهرها وبذلك لا يشك أحد في أن هناك معلومات حساسة يتم تهريبها حتى ولو تم ضبط الشخص متلبساً، كما قد يلجأ إلى وسائل غير تقليدية للحصول على المعلومات السرية [2] وبعد الاعتداءات الأخيرة على الولايات المتحدة الأمريكية صدرت تعليمات جديدة لأقمار التجسُّس الاصطناعية الأمريكية بالتركيز على أفغانستان والبحث عن أسامة بن لادن والجماعات التابعة له، وقررت السلطات الأمريكية الاستعانة في عمليات التجسُّس على أفغانستان بقمرين اصطناعيين عسكريين مصممان خصيصاً لالتقاط الاتصالات التي تجري عبر أجهزة اللاسلكي والهواتف المحمولة، بالإضافة لقمرين اصطناعيين آخرين يلتقطان صورا فائقة الدقة وفي نفس الوقت طلب الجيش الأمريكي من شركتين تجاريتين الاستعانة بقمرين تابعين لهما لرصد الاتصالات ومن ثم تحول بعد ذلك إلى الولايات المتحدة حيث تدخل في أجهزة كمبيوتر متطورة لتحليلها. وتُشارك في تلك العمليات شبكة إشيلون المستخدمة في التجسُّس على المكالمات الهاتفية ورسائل الفاكس والبريد الإليكتروني، الأمر الذي يُتيح تحليل الإشارات التي تلتقطها الأقمار الصناعية حتى إن كانت واهنة أو

---

(1) Cybercrime: Law Enforcement, Security, and Surveillance in the Information Age, by Tom Douglas Brian Loader. Thomas Douglas, 1st edition) Routledge, 2000.

(2) Tom forester, Essential problems to High-Tech Society First MIT Pres edition, Cambridge, Massachusetts, 1989, p 104.

مشفرة (BBC,2001).

نص نظام مكافحة جرائم المعلوماتية السعودي رقم 79 الصادر بتاريخ 1428/3/7 هـ على عقوبة تلك الجريمة في المادة الثالثة فقرة 1:

يُعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية: «التصنت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي – دون مسوّغ نظامي صحيح – أو التقاطه أو اعتراضه».

المبحث الخامس

الإرهاب الإليكتروني

في عصر التقدم الإليكتروني وفي زمن قيام حكومات إليكترونية، تبدل نمط الحياة وتغيرت معه أشكال الأشياء وأنماطها ومنها ولا شك أنماط الجريمة والتي قد يحتفظ بعضها بمسماها التقليدي مع تغيير جوهري أو بسيط في طرق ارتكابها، ومن هذه الجرائم الحديثة في طرقها القديمة في اسمها جريمة الإرهاب والتي أخذت منحنى حديث يتماشى مع التطور التقني[1]. وقد انتبه الغرب إلى قضية الإرهاب الإليكتروني منذ فترة مبكرة، فقد شكّل الرئيس الأمريكي بيل كلنتون لجنة خاصة (www.nipc.gov) مهمتها حماية البنية التحتية الحساسة في أمريكا، والتي قامت في خطوة أولى بتحديد الأهداف المحتملة استهدافها من قِبل الإرهابين ومنها مصادر الطاقة الكهربائية والاتصالات إضافة إلى شبكات الحاسب الآلي، ومن ثم تم إنشاء مراكز خاصة في كل ولاية للتعامل مع احتمالات أي هجمات إرهابية إليكترونية. كما قامت وكالة الاستخبارات المركزية بإنشاء مركز حروب المعلوماتية وظفت به ألفاً من خبراء امن المعلومات، كما شكلت قوة ضاربة لمواجهة الإرهاب على مدار الساعة ولم يقتصر هذا الأمر على هذه الوكالة بل تعداه إلى الأجهزة الحكومية الأخرى كالمباحث الفيدرالية والقوات الجوية. وحذّرت وزارة الدفاع الأمريكية عام (1997م) من ((بيرل هاربور إليكترونية)) وتوقع التقرير أن يزداد الهجوم على نظم المعلومات في الولايات المتحدة الأمريكية من قبل الجماعات الإرهابية أو عملاء المخابرات الأجنبية وأن يصل هذا الهجوم إلى ذروته عام (2005م)، وأوضح التقرير أن شبكة الاتصالات ومصادر الطاقة الكهربائية والبنوك وصناعات النقل في أمريكا

---

(1) ياسين، صباغ محمد محمد، الجهود الدولية والتشريعية لمكافحة الإرهاب وقرب العالم الجديد، دار الرضوان، القاهرة، 2005م.

معرَّضة للهجوم من قِبل أي جهة تسعى لمحاربة الولايات المتحدة الأمريكية دون أن تواجه قواتها المسلحة [1] وبعد الهجمات الأخيرة على الولايات المتحدة الأمريكية ارتفعت أصوات البعض بممارسة الإرهاب الإليكتروني ضد المواقع الإسلامية والعربية التي يشتبه بأنها تدعم الإرهاب، وتناول نظام مكافحة جرائم المعلوماتية السعودي رقم 79 الصادر بتاريخ 1428/3/7 هـ النص على عقوبة تلك الجريمة في المادتين السابعة والثامنة:

المادة السابعة:

يُعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

1 - إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها أو ترويج أفكارها أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أداة تستخدم في الأعمال الإرهابية.

2 - الدخول غير المشروع إلى موقع إليكتروني، أو نظام معلوماتي مباشرة، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني.

المادة الثامنة:

لا تقل عقوبة السجن أو الغرامة عن نصف حدها الأعلى إذا اقترنت

(1) جيشن وآخرون، بيل، المعلوماتية بعد الانترنت (طريق المستقبل)، ترجمة رضوان، عبد السلام، سلسلة عالم المعرفة، المجلس الوطني للثقافة والفنون الآداب، العدد 231، الكويت، مارس 1988م.

الجريمة بأي من الحالات الآتية:

1 - ارتكاب الجاني الجريمة من خلال عصابة منظمة.

2 - شغل الجاني وظيفة عامة، واتصال الجريمة بهذه الوظيفة، أو ارتكابه الجريمة مستغلاً سلطاته أو نفوذه.

3 - التغرير بالقصر ومَن في حكمهم، واستغلالهم.

4 - صدور أحكام محلية أو أجنبية سابقة بالإدانة بحق الجاني في جرائم مماثلة.

المبحث السادس

جريمة انتحال الشخصية عبر الانترنت

توجد الكثير من البرامج التي تمكن المستخدم من إخفاء شخصيته سواء أثناء إرسال البريد أو أثناء تصفُّح المواقع. ولا شك أن أغلب مَن يستخدم هذه البرامج هدفهم غير نبيل، فيسعون من خلالها إلى إخفاء شخصيتهم خوفاً من مسائلة نظامية أو خجلاً من تصرُّف غير لائق يقومون به. ومن الأمور المسلمة بها شرعاً وعرفاً أن الأفعال الطيبة لا يخجل منها الأشخاص بل يسعون عادة، إلا في حالات معينة، إلى الإعلان عنها والافتخار بها، أما الأفعال المشينة فيحرص الغالبية على إخفائها. فإخفاء الشخصية غالباً أمر مشين وتهرُّب من المسئولية التي قد تلحق بالشخص متى ما عرفت شخصيته، ولعل ما يدل على ذلك حديث رسول الله ﷺ «البر حسن الخلق، والإثم ما حاك في صدرك وكرهت أن يطلع عليه الناس»[1].

انتحال الشخصية: وهي تنقسم إلى قسمين:

أ - **انتحال شخصية الفرد:** تُعتبر جرائم انتحال شخصية الآخرين من الجرائم القديمة إلا أن التنامي المتزايد لشبكة الانترنت أعطى المجرمين قدرة أكبر على جمع المعلومات الشخصية المطلوبة عن الضحية والاستفادة منها في ارتكاب جرائمهم. فتنتشر في شبكة الانترنت الكثير من الإعلانات المشبوهة والتي تداعب عادة غريزة الطمع الإنساني في محاولة الاستيلاء على معلومات اختيارية من الضحية، فهناك مثلاً إعلان عن جائزة فخمة يكسبها مَن يساهم بمبلغ رمزي لجهة خيرية والذي يتطلب بطبيعة الحال الإفصاح عن بعض المعلومات الشخصية كالاسم

---

(1) رواه مسلم

والعنوان والأهم رقم بطاقة الائتمان لخصم المبلغ الرمزي لصالح الجهة الخيرية، وبالرغم من أن مثل هذا الإعلان من الوضوح بمكان أنه عملية نصب واحتيال إلا أنه ليس من المستبعد أن يقع ضحيته الكثير من مستخدمي الانترنت. ويمكن أن تؤدي جريمة انتحال الشخصية إلى الاستيلاء على رصيده البنكي، أو السحب من بطاقته الائتمانية، أو حتى الإساءة إلى سمعة الضحية[1].

ب - **انتحال شخصية المواقع:** مع أن هذا الأسلوب يعتبر حديث نسبياً، إلا أنه اشد خطورة وأكثر صعوبة في اكتشافه من انتحال شخصية الأفراد، حيث يمكن تنفيذ هذا الأسلوب حتى مع المواقع التي يتم الاتصال بها من خلال نظم الاتصال الآمن (Secured Server) حيث يمكن وبسهولة اختراق مثل هذا الحاجز الأمني، وتتم عملية الانتحال بهجوم يشنه المجرم على الموقع للسيطرة عليه ومن ثم يقوم بتحويله كموقع بيني، أو يحاول المجرم اختراق موقع لأحد مقدمي الخدمة المشهورين ثم يقوم بتركيب البرنامج الخاص به هناك مما يؤدي إلى توجيه أي شخص إلى موقعه بمجرد كتابة اسم الموقع المشهور. ويتوقع أن يكثر استخدام أسلوب انتحال شخصية المواقع في المستقبل نظراً لصعوبة اكتشافها [2].

والمحاذير الأمنية والمخالفات النظامية والشرعية واضحة في هذه الفقرة سواء ما كان منها قاصراً على انتحال شخصية الأفراد أو المواقع، فقد حفظت الشريعة السماوية والأنظمة الوضعية الحقوق الشخصية وصانت الملكيات الفردية وجعل التعدي عليها أمراً محظوراً شرعياً ومعاقَب عليه

(1) الخليل، عماد علي، التكييف القانوني لإساءة استخدام أرقام البطاقات عبر شبكة الانترنت، المرجع السابق.

(2) عرب، يونس، صور الجرائم الإليكترونية واتجاهاتها تبويبها ورقة عمل سنة 2006م.

جنائياً. وفي انتحال شخصية الآخرين تعدّي صارخ على حقوقهم وانتهاكاً لمكياتهم التي صانها الشرع لهم، كما أنه ترتّب على انتحال شخصية الآخرين أضرار متنوعة قد تلحق بهم، وتتفاوت هذه الأضرار بتفاوت نتيجة الفعل والذي قد تقتصر على أضرار معنوية كتشويه سمعة الشخص وقد تصل إلى أضرار مادية كالاستيلاء غير المشروع على ممتلكات ومقتنيات مادية للمجني عليه. ومهما كان حجم هذه الأضرار الناتجة عن هذا الفعل غير النظامي فإنه لا يمكن إلا أن يتضرر المجني عليه من هذا الفعل وخاصة أن الهدف الغالب من وراء انتحال الشخصية لن يكون حميداً، أو بحسن نية، أو لخدمة شخص آخر خلاف منتحل الشخصية. وتتفق الشريعة مع القوانين الوضعية في جعل الإنسان مسئولاً عن كل فعل ضار بغيره، سواء اعتبر القانون ذلك الفعل جريمة أم لم يعتبره [1] ولا شك أن انتحال شخصية الأفراد أو المواقع مضر بأصحابها الأساسيين؛ ولذلك فهي جريمة قانونية ومخالفة شرعية. وتناول نظام مكافحة جرائم المعلوماتية السعودي رقم 79 الصادر بتاريخ 1428/3/7 هـ النص على عقوبة تلك الجريمة في **المادة الرابعة**: يُعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيّاً من الجرائم المعلوماتية الآتية:

1 - الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة.

2 - الوصول - دون مسوّغ نظامي صحيح - إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات.

---

(1) عرب، يونس، جرائم الكمبيوتر والانترنت، موسوعة القانون وتقنية المعلومات، منشورات اتحاد المصارف العربية، الطبعة الأولى، الجزء الثاني، 2002م.

المبحث السابع

سرقة الملكية الفكرية

«الملكية الفكرية هي: حقوق امتلاك شخص ما لأعمال الفكر الإبداعية أي الاختراعات والمصنفات الأدبية والفنية والرموز والأسماء والصور والنماذج والبرامج والرسوم الصناعية، التي يقوم بتأليفها أو إنتاجها» [1].

يمكن تصنيف مكوّنات وحقوق الملكية الفكرية إلى مجموعتين:

1 - **مكوّنات الملكية الفكرية التقليدية:** وهي المكوّنات والحقوق المعروفة وتتمتع بالحماية وهي: الأسرار التجارية، والبراءة، والعلاقة التجارية، وحق النشر.

2 - **المكوّنات والحقوق الرقمية للملكية الفكرية:** ظهرت في ظل الانترنت، ذات طبيعة رقمية وتشمل البرمجيات، قواعد البيانات، والمواقع الإليكترونية وغيرها.

وهذا النوع الأخر من حقوق الملكية الفكرية ألا وهو الحقوق الرقمية والذي يشمل:

1 - البرمجيات:

البرمجية (Software) خلاف الأجهزة (Hardware) فالبرمجيات هي الأساس الذي تعمل من خلاله الأجهزة لتحويلها إلى شئ مفيد يقوم بوظائف عدة مثل أنظمة التشغيل، وهي من أكبر الأمثلة على البرمجيات. وعلى الرغم من أن البرمجيات (بنوعيها برمجيات النظام وبرمجيات التطبيق) كانت موجودة قبل الانترنت والاستخدام التجاري الواسع لشبكات الأعمال، إلا

---

(1) راجع الرابط www. mawhiba. org/EBTEKAR/... 0../sdetail. aspx

أنها أصبحت في ظل الانترنت تُشكل القدرة الفكرية والخبرة العظيمة التي تُحرك اقتصاد المعلومات كله والمصدر الأكثر فعالية وكفاءة في صنع الثروة في الأعمال الإليكترونية.

والبرمجيات هي من أكثر المنتجات الرقمية حاجة للحماية؛ لأنها الأكثر عرضة للقرصنة.

2 - قرصنة البرمجيات:

هي أن تقوم بنسخ البرامج واستخدامها بدون دفع ثمنها للشركة أو الشخص الذي قام بتصنيعها؛

فالحل البديل لقرصنة البرمجيات هو استخدام البرمجيات الحرة. البرمجيات حرة المصدر هي البديل الأمثل للبرمجيات المقرصنة إن لم تود أن تدفع ثمن البرامج الأصلية. وهي برمجيات يمكن استخدامها والتعديل بها وإعادة توزيعها مجاناً بدون أي مقابل مادي بشرط عدم نسبها لأحد غير صاحبها الأصلي.

ويوجد برمجيات حرة المصدر ذات مستوى عالي من الكفاءة ويوجد أيضاً بديل حر المصدر لكل البرامج التي يقوم المستخدمين بقرصنتها فمثلاً بدل من نظام تشغيل وندوز.

يوجد نظام تشغيل لينكس وبدلاً من حزمة الأوفيس يوجد حزمة الأوبن أوفيس وبدل من متصفِّح انترنت اكسبلورر يوجد متصفِّح فاير فوكس وبدل من برنامج الأدوب فوتوشوب يوجد برنامج جيمب، فهذه هي فكرة البرمجيات حرة المصدر.

3 - قواعد البيانات الإليكترونية:

من المفترض حفظ قواعد البيانات من الاستنساخ واستغلال الآخرين

فلابد أن تكون محمية بقوانين حفظ الملكية شأنها شأن أي عمل آخر. وأيضاً من الممكن حمايتها بما يُسمَّى بحق قاعدة البيانات (Database Right).

4 - الموقع الإليكتروني:

الموقع الإليكتروني هو: عبارة عن مجموعة من صفحات الويب ذات الصلة مع بعضها البعض، يمكن الوصول إليها عبر شبكة مثل الانترنت أو الشبكة المحلية الخاصة.

والصفحة الواحدة تحتوي على نص، أو صور، أو مقاطع فيديو وغيرها. وهذه الصفحة ممكن أن تُشارك في الإقناع والشراء والبيع وأغراض أخرى لا تقل أهمية عن هذه الأمور، لذا لابد أن تكون محمية بالحماية القانونية التي لا تزال غير معترَف بها لمثل هذه المواقع.

إن سرقة وقت الانترنت يأتي في إطار القرصنة (hacking) وهو استخدام من قِبل شخص غير مصرَّح به لساعات للانترنت المدفوعة من قبل شخص آخر، فالقرصان يصل إلى كلمة المرور للوصول إلى الانترنت إما عن طريق القرصنة (Internet Identity Theft) أو عن طريق وسائل غير قانونية، فيصل إلى الانترنت من دون علم أو معرفة الشخص الآخر. ونعرف أن الوقت تمت سرقته من قِبل أي قرصان عندما ينتهي شحن الوقت ونحتاج إلى تعبئتها أو شحنها مع العلم أن الشخص لا يستخدمها بكثرة !!

إن السارق يصل إلى كلمة المرور للوصول إلى الانترنت حيث أن جهاز الكمبيوتر - مما لا نعرف عنه - أنه يقوم بجمع جميع أنواع المعلومات ويخزِّنها في الملفات المخفية على القرص الصلب. وهذه الملفات تقوم بتخزين المعلومات مثل تسجيل الدخول وكلمات السر، والأسماء والعناوين وحتى أرقام بطاقات الائتمان. ويمكن الحصول على هذه المعلومات بطريقتين: إما عن طريق الاستيلاء عليها أثناء انتقالها انتقالاً غير آمن بين الأجهزة عبر الشبكة، أو

عن طريق تثبيت برامج ضارة على جهاز الكمبيوتر الخاص بك (مثل برامج التجسُّس) التي من شأنها أن تجمع كل شئ تحتاج إليه تلقائياً وإعادتها إلى الجهاز مرة أخرى. وأفضل طرق الحماية من هذا النوع [1]:

- تأمين متصفّح الويب.
- حماية المعلومات الحساسة والخاصة.
- حذف محفوظات المواقع على الانترنت.
- حذف ذاكرة التخزين المؤقتة الخاصة بك على الجهاز.
- إفراغ سلة المحذوفات.

---

(1) عرب، يونس، جرائم الكمبيوتر والانترنت، المركز العربي للدراسات والبحوث الجنائية، ابو ظبي 10-2002/2/12م.

المبحث الثامن

المسئولية الجنائية للجرائم المعلوماتية

المطلب الأوّل

المسئولية الجنائية لوسطاء تقديم خدمات شبكة الانترنت

يتمثّل أساس المسئولية الجنائية في الالتزام القانوني بتحمُّل التبعة فهي تنشأ تابعة لالتزام آخر وهو في حقيقته واجب أصلي. فللمسئولية الجنائية ركنان أساسيان، الأول هو علاقة السببية بين السلوك الإجرامي والنتيجة أي الإسناد المادي من جهة، والثاني هو الرابطة المعنوية بين الشخص والسلوك، فإذا كانت القاعدة العامة في أساس المسئولية الجنائية شخصية، وكان كل إنسان لا يسأل إلا عن أعماله وسلوكه، فلو نظرنا للمشرّع الليبي أسوة بغيره من المشرّعين خرج عن هذه القاعدة وأخذ بالمسئولية الجنائية عن الغير في مجال النشر، فأخذ بالمسئولية الجنائية المفترَضة على أساس تضامني يتمثّل في افتراض علم رئيس التحرير بالمضمون المنشور في الصحيفة واعتباره الفاعل الأصلي في الجرائم المرتكبة بواسطة النشر، وهي المسئولية الجنائية المفترضة على أساس تضامني استناداً إلى علم رئيس التحرير بالمضمون المنشور في الصحيفة واعتباره الفاعل الأصلي وكل مَن يُساهم فيها بعد فاعلاً أو شريكاً حسب القواعد العامة بحيث لا يسأل شخص بينهم ما دام يوجد من قدمه عليه القانون في ترتيب المسئولية الجنائية وهي ما تُسمى بالمسئولية المتتابعة [1].

---

(1) عرب، يونس، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، منشورات إتحاد المصارف العربية، الطبعة الأولى 2000م.

ومع مراعاة مسئولية المؤلف وباستثناء حالات الاشتراك إذا ارتكبت إحدى الجرائم عن طريق الصحافة الدورية يُعاقب حسب الأحكام الآتية: المدير أو المحرر المسئول الذي لا يمنع النشر عندما لا تتوفر الموانع الناتجة عن القوة القاهرة، أو الحادث الطارئ، أو الإكراه المادي، أو المعنوي الذي لا يمكن دفعه إذا كّون الفعل جناية أو جنحة تتوفر فيها النية الإجرامية وتُطبق العقوبة المقررة للجريمة المرتكبة مع خصمها إلى حد النصف وإذا كوّن الفعل جريمة خطيئة أو مخالفة فتطبق العقوبة المقرر لها)، والمسئولية المتابعة بالنسبة للجرائم المرتكبة بواسطة المطبوعات غير الدورية أو شبه الدورية[1].

فكرة المسئولية المتابعة تقوم على ترتيب الأشخاص المسئولين جنائياً وحصرهم بحيث لا يسأل واحد منهم إلا إذا لم يوجد غيره ممن قدمه القانون عليه في الترتيب حتى نصل إلى الطابع.

أما نوع المسئولية الجنائية لوسطاء تقديم خدمات شبكة الانترنت فإذا كانت شبكة الانترنت وسيلة من وسائل النشر والعلانية مما لا تثور معه صعوبة في إمكانية تطبيق الأحكام القانونية لجرائم السب والتشهير، فإن الجدل القانوني يثور بالنسبة لتحديد المسئولين جنائياً عن السلوك المرتكب في الفضاء الإليكتروني وحصر المساهمين فيه، فمن هم الأشخاص القائمين على تشغيل الشبكة وخدماتها المتعددة؟.

لقد أصبحت الشبكة العالمية اليوم تضم مجموعة من الأنشطة والخدمات المختلفة فهي بنية تحتية للاتصالات أهم خدماتها البريد الإليكتروني والمنتديات والناقل لنقل الملفات بين أرجاء الشبكة، ووسيلة المتصل، وهو البرنامج الذي يُتيح لأي شخص استخدام برامج ومميزات حاسوبية موجودة في جهاز آخر بعيد ولا توجد في جهاز المستخدم، أما شبكة المعلومات الدولية فهي إحدى

---

(1) عبادة، عبادة أحمد، التدمير المتعمد لأنظمة المعلومات الإليكترونية مركز البحوث والدراسات، شرطة دبي بدولة الإمارات العربية المتحدة 2005 م.

خدمات الشبكة من صفحات مصححة بلغة HTML التي تُتيح إمكانية ربط الصفحات بالوسائط وهو سر تسميتها بالشبكة العنكبوتية [1].

ويمكن أن نعرف مزود الخدمة بأنه كل شخص يمد المستخدمين بالقدرة على الاتصال بواسطة أنظمة الحاسب الآلي أو يقوم بمعالجة البيانات وتخزينها بالنيابة عن هؤلاء المستخدمين: وهو ما نصت عليه المادة (1) (2) من اتفاقية بوداست 2001 بشان جرائم الإنترنت، فمزود الخدمة هو مَن يمكن المشتركين من الوصول إلى شبكة الانترنت عن طريق مدهم بالوسائل الفنية اللازمة للوصول إلى الشبكة بمقتضى عقد توصيل الخدمة، فهو لا يقوم بتوريد المعلومة أو تأليفها، ولا يملك أي وسائل فنية لمراجعة مضمونها، لأن دوره فني يتمثّل في نقل المعلومات على شكل حزم إليكترونية عن طريق حاسباته الخادمة، فهل يجوز اعتباره أحد المسئولين على الجريمة المعلوماتية؟

المطلب الثاني

اتجاهات الفقه حول مسئولية مزود الخدمة

تبيَّنت واختلفت الآراء حول مسئولية مزود الخدمة إلى الاتجاهات الآتية

أولاً: الاتجاه القائل بعدم مسئولية المزود:

لقد استند هذا الاتجاه إلى أن مزود الخدمة لا يملك القدرة على التحكم في أي مضمون يبث على الشبكة، والقول بتقرير مسئوليته هنا يناظر القول بمساءلة مدير مكتب البريد والهواتف على مدى مشروعية الخطابات

(1) اللحيدان، فهد بن عبدالله، الانترنت، شبكة المعلومات العالمية، الطبعة الأولى، الناشر غير معروف، 1996م.

والمكالمات التي تجري عبر هذه الخطوط [1] بل إن المسألة قد تنتهي بنا إلى تقرير مسئولية الجهات العامة على توفير محطات التقوية لبث القنوات الفضائية المرئية. فتقرير مسئولية مزود الخدمة يتطلّب أن يكون دوره أكثر إيجابية في بث المادة المجرمة بالإضافة إلى أنه لا يملك الوسائل الفنية التي تُمكنه من مراقبة تلك المعلومات المتدفقة بأعداد تتجاوز الملايين [2].

ثانياً: الاتجاه القائل بتقرير مسؤولية مزود الخدمة:

انقسم أنصارها الاتجاه إلى فريقين: الأول ينادي بتقرير المسئولية الجنائية طبقاً لأحكام المسئولية المتتابعة، والثاني يذهب إلى تقرير المسئولية طبقاً للأحكام العامة للمسئولية الجنائية.

المطلب الثالث

مساءلة مزود الخدمة طبقاً لأحكام المسئولية المتتابعة

يبدو لأول وهلة استجابة الدور الذي يقوم به مزود الخدمة لهذا النظام استناداً إلى مساهمته في عملية النشر وتحقيق العلانية ووضعها في متناول المستخدمين.

إلا أن المسئولية المتتابعة في مجال النشر بالنسبة للمؤلف والناشر تقوم على أساس العلم المسبق بما تم إعلانه ونشره للآخرين وهو ما يوجب التزام الناشر أو رئيس التحرير بالمراقبة مما لا يتوفر بالنسبة لمزود الخدمة، خاصة عند قيامه بالربط أثناء المنتديات المختلفة حيث يقوم بتثبيت تلك المؤتمرات

(1) الصغير، جميل عبد الباقي، الانترنت والقانون الجنائي، دار النهضة العربية، 1992م.

(2) رمضان، مدحت، جرائم الاعتداء على الاشخاص والانترنت، دار النهضة العربية، القاهرة، 2000م.

على جهازه الخادم وكل ما يصل لمزود الخدمة في هذه الحالات هي حزم من البيانات المشفرة [1].

وهو ما نصل معه إلى عدم قبول تطبيق أحكام المسئولية المتابعة لأن مزود الخدمة لا يملك الوسائل الفنية والقانونية التي تمكّن من مراقبة المضمون الذي ينشر ويتحرك على الشبكة.

الفرع الأوّل

مساءلة المزود طبقاً للأحكام العامة للمسئولية الجنائية

يستند أصحاب هذا الرأي إلى أن مزود الخدمة لا يملك الوسائل الفنية اللازمة لمراقبة الصورة أو الكتابة إلا أنه يملك الوسائل الفنية اللازمة لمنع الدخول إلى هذه المواقع مما يؤدي إلى تقديم المساعدة لأصحاب تلك المواقع عن طريق مدهم بالزائرين وهو ما تتحقق به المساهمة الجنائية التبعية بالمساعدة [2].

لكن يُعد هذا الرأي أيضاً محل نظر؛ لأن المساهمة الجنائية طبقاً لأحكام القانون الجنائي الليبي لا تكون إلا بالأعمال السابقة أو المعاصرة للسلوك الإجرامي ولا تكون بالأعمال اللاحقة [3]. أما مزود الخدمة فدوره يأتي لاحقاً لارتكاب الجريمة التي تحقّقت بكامل عناصرها على الشبكة قبل أن يبدأ دور مزود الخدمة [4].

---

(1) منصور، محمد حسن، المسئولية الإليكترونية، المرجع السابق.

(2) اللحيدان، فهد بن عبدالله، الانترنت، شبكة المعلومات العالمية، المرجع السابق.

(3) الصغير، جميل عبد الباقي، الانترنت والقانون الجنائي، المرجع السابق.

(4) منصور، محمد حسن، المسئولية الإليكترونية، المرجع السابق.

هكذا نصل إلى صعوبة تطبيق فكرة العلم المسبق لأسباب فنية وقانونية، فالأسباب الفنية تتمثل في عدم وجود الإمكانية لمراقبة المضمون المنشور قبل نشره، أما الأسباب القانونية فترجع إلى عدم اختصاص مزود الخدمة بممارسة أي نوع من أنواع الرقابة التوجيهية على ما يتم نشره لما في ذلك من تعارض والعديد من الضمانات الخاصة بحق المؤلف وحق الحياة الخاصة، ولا يمكن قبول قيامها بأي دور وقائي على الآخرين.

الفرع الثاني

المسئولية الجنائية لمتعهد الاستضافة عبر الانترنت

متعهد الاستضافة هو شخص يتولى إيواء صفحات معنية من الشبكة (WEB) على حساباته الخادمة مقابل أجر معين على الشبكة، حيث يقوم العميل وهو بمثابة المستأجر لتلك المساحة بكتابة المضمون الخاص عليها بطريقة مباشرة فيقوم بتخزين المادة المنشورة [1] والمادة المعلوماتية لكي يتمكن العميل من الوصول إليها في أي وقت [2] كما يتولى مهمة تخزين وإدارة المحتوى الذي قدمه له العميل فهو يساهم في عملية النشر دون أن يكون بإمكانه السيطرة على المعلومة أو المضمون المنشور قبل عرضه على الانترنت، فهو يساعد المستخدم في الوصول إلى الموقع والتجول فيه.

والآراء تتبين حول تقرير المسئولية لعمال الإيواء كما يلي:

---

(1) عفيفي، عفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، 2003.

(2) منصور، محمد حسن، المسئولية الإليكترونية، المرجع السابق.

أولاً: القول بعدم مسئولية عامل الإيواء:

يطلب عاملو الإيواء إعفاءهم من المسئولية الجنائية استناداً إلى أنهم يقومون بدور فني يتمثل في إيواء المعلومة وتخزينها لتمكين الجمهور من الاطلاع عليها وهو ما أخذ به المشرِّع الفرنسي في القانون رقم 719 الصادر سنة 2000 م بتعديل قانون حرية الاتصالات، فنص التعديل على انتفاء المسئولية الجنائية والمدنية بالنسبة لكل الأشخاص الطبيعيين أو المعنويين الذين يتعهدون بالتخزين المباشر والمستمر من أجل أن يضعوا تحت تصرف الجمهور إشارات، أو كتابات، أو صور، أو رسائل، ولم يلزمهم هذا القانون إلا بضرورة التحقق من شخصية المساهم في وضع المضمون أو كتابته ويستند أنصار هذا الاتجاه إلى أن دور التخزين الذي يقوم به عامل الإيواء لا يسمح بالسيطرة على المضمون [1]

ثانياً: القول بمساءلة عامل الإيواء:

واجه الرأي السابق نقداً شديداً وذهب رأي آخر إلى أن عامل الإيواء يجب أن يكونَ مسئولاً؛ لأنه بإمكانه رفض عملية الإيواء إذا شعر بعدم مشروعية المضمون المنشور [2].

المطلب الرابع

المسئولية الجنائية طبقاً للأحكام العامة للمساهمة الجنائية

إذا كان عامل الإيواء يقوم باستضافة المعلومة أو المضمون المنشور على صفحاته دون أن يكون لديه أي سيطرة على المضمون، فسلطته على هذا

(1) الصغير، جميل عبد الباقي، الانترنت والقانون الجنائي، المرجع السابق.

(2) منصور، محمد حسن، المسئولية الإليكترونية، المرجع السابق.

الأخير وعلمه به يُشبه مدى علم المؤجر بالجرائم التي يرتكبها المستأجر في العين المؤجرة وفي هذه الحالة تنتفي المسئولية الجنائية لعامل الإيواء بمجرد ثبوت عدم علم عامل الإيواء بالمضمون غير المشروع، خاصة وأن البيانات والمعلومات تتدفق بين أرجاء الشبكة بسرعة الضوء، وهو ما يتضح بصورة واضحة في المنتديات ومجموعات المناقشة، أما بالنسبة لباقي الجرائم المرتكبة عبر صفحات (WEB) فإنها من الجرائم المستمرة إلى يستمر ارتكابها باستمرار عرضها على الصفحة ما يعني إمكانية نشوء قرينة على العلم لها، وهنا يكون على المشرّع الليبي عند صياغة الأحكام العامة للمسئولية الجنائية للمستضيف أن يقوم بأعمال الموازنة بين التزامات هذا الأخير بعدم عرض المعلومات غير المشروعة من جهة حقوق المؤلف بالنسبة لصاحب المعلومة من جهة أخرى[1].

إن صعوبة تطبيق الأحكام العام على أي من الوسيطين لصعوبة إثبات العلم بالمضمون المجرم مما تنتفي معه الوحدة لمعنوية بين المساهمين أما أحكام المسؤولية المتابعة فلا يمكن تطبيقها أيضاً لا لصعوبة مراقبة المضمون فحسب بل لاعتبار آخر لا يقل أهمية وهو أن أحكام المسئولية المتابعة استثناء من الأصل العام لا يجوز التوسع فيه.

فالمسئولية الجنائية يجب أن تتقرر بنص صريح ويجب أن ترتبط بإمكانية السيطرة على المعلومة فالوسيط في تقديم هذه الخدمات سواءً كان مزود الخدمة أو عامل الإيواء، عبارة عن وسيط تجاري يقوم بأعمال الوسائط في CYBER SPACE وهو ما يميزه عن الوسيط التقليدي الذي يكون قريباً من الأطراف وأكثر قدرة على تقييم تصرفاتهم بينما الوسيط المعلوماتي يقوم بدور الوسيط في بيئة افتراضية تنعدم فيها الحدود الجغرافية اللازمة للاقتراب والتقييم كما تنعدم فيها النظم القانونية الحاكمة من جهة أخرى[2].

---

(1) الصغير، جميل عبد الباقي، الانترنت والقانون الجنائي، المرجع السابق.

(2) Chriss Reed, Internet Law, 2004, CAMPRIDGE UNIVERCITY PRESS. p 89.

من الذي يرتكب جرائم الكمبيوتر وما هي دوافعهم؟؟ ليس ثمة أصدقاء في العالم الإليكتروني، وصغير المجرمين ككبيرهم، والمازح من بينهم كالحاقد، وضمان أمن المعلومات وضمان عدم التعرُّض للمسئوليات يوجب التعامل مع الكل على أنهم مصدر للخطر، وليست المسالة إهداراً لفكرة حسن النية أو الثقة بالآخرين، إنها الضمان الوحيد للحماية من مصادر خطر بالغة قد تودي إلى مسئوليات وخسائر لا يمكن تقديرها أو تجاوزها. ما من شك أن المدى الزمني لنشأة وتطور العلوم الجنائية، حمل معه نشوء وتطور واندثار نظريات عدة في مجال علم الإجرام، وفي مجال تصنيف المجرمين، وأسباب الجنوح والانحراف، وأمكن في ظل هذه العلوم، وما نتج في نطاقها من دراسات، في ميدان علم الإجرام تحديداً، بلورة سمات عامة للمجرم عموماً، وسمات خاصة يمكن استظهارها لطائفة معينة من المجرمين، تبعاً للجرائم التي يرتكبونها، فعلى سبيل المثال، أفرزت الجرائم الاقتصادية ما يعرف بإجرام ذوي الياقات البيضاء. وبالتالي، كان طبيعياً أن تحمل ظاهرة جرائم الحاسب في جنباتها ولادة طائفة من المجرمين، مجرموا الحاسب، تتوافر فيهم سمات عامة بغض النظر عن الفعل المرتكب، وسمات خاصة تبعا للطبيعة المميزة لبعض جرائم الحاسب، والأغراض المراد تحقيقها. والحقيقة أنه، وحتى الآن، لم تتضح الصورة جلية في شأن تحديد صفات مرتكبي جرائم الحاسب، واستظهار سماتهم، وضبط دوافعهم، نظراً لقلة الدراسات الخاصة بالظاهرة برمتها من جهة، ونظراً لصعوبة الإلمام بمداها الحقيقي، بفعل الحجم الكبير من جرائمها غير المكتَشف، أو غير المبلغ عن وقوعها، أو التي لم تتم بشأنها ملاحقة قضائية رغم اكتشافها، لصعوبة إثباتها أو للنقص التشريعي الذي يحدُّ من توفير الحماية الجنائية في مواجهتها. في بداية الظاهرة شاع الحديث عن المجرمين الصغار الذين يرتكبون مختلف أنواع الاعتداءات على نظم الكمبيوتر وتحديداً الاختراقات بدافع التحدي وإثبات المقدرة العلمية والتقنية؛ وكان ثمة حديث عن استغلال منظمات الجريمة لهؤلاء النابغين وتحديداً استغلال

ميول التحدي لديهم وأحياناً احتياجاتهم المادية لتسخيرهم للقيام بأنشطة إجرامية تتصل بالتقنية تدر منافع لمنظمات الجريمة، ومع تنامي الظاهرة وتعدد أنماط هذه الجرائم، ونشوء أنماط جديدة متصلة بشبكات الكمبيوتر وتحديداً الانترنت (1)، اتجهت جهات البحث وتحديداً الهيئات العاملة في ميدان السلوك الإجرامي لمحاولة تصنيف مرتكبي جرائم الكمبيوتر والانترنت وبيان السمات الأساسية لكل فئة بغرض بحث أنجح الوسائل لردع هذه الفئات أو الحد من نشاطها، باعتبار ذلك من المسائل الموضوعية اللازمة لتحديد اتجاهات المكافحة. إن دراسات علم الإجرام الحديثة في ميدان إجرام التقنية تسعى في الوقت الحاضر إلى إيجاد تصنيف منضبط لمجرمي التقنية لكنها تجد صعوبة في تحقيق ذلك بسبب التغير السريع الحاصل في نطاق هذه الظاهرة والمرتبط أساساً بالتسارع الرهيب في ميدان الكمبيوتر والانترنت، فالمزيد من الوسائل والمخترعات والأدوات التقنية يساهم في تغير أنماط الجريمة وتطور وفعالية وسائل الاعتداء، وهذا بدوره يُساهم في إحداث تغيرات على السمات التي يتصف بها مجرمي التقنية، على الأقل السمات المتصلة بالفعل نفسه وليس بالشخص (2)، ولهذا يتجه الباحثون مؤخراً إلى الإقرار بأن أفضل تصنيف لمجرمي التقنية هو التصنيف القائم على أساس أغراض الاعتداء وليس على أساس التكنيك الفني المرتكب في الاعتداء أو على أساس الوسائط محل الاعتداء أو المستخدمة لتنفيذه(3).

إن طريق الدفاع الأول ضد جرائم الكمبيوتر والانترنت هو توعية الأفراد والمؤسسات بأهمية اتخاذ الأدوات والسياسات المناسبة لتفادي

(1) عرب، يونس، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، المرجع السابق.

(2) الجنبيهي، منير، والجنبيهي، ممدوح، صراخ الانترنت وسائل مكافحتها، 2005 م، دار الفكر الجامعي، الإسكندرية.

(3) عرب، يونس، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، المرجع السابق.

جرائم الانترنت، وضرورة وضع برامج التوعية الإعلامية لرفع الوعي الأمني للمعلومات والممتلكات الالكترونية.

جرائم الإنترنت لم يكن هناك قلق مع بدايات شبكة الإنترنت تجاه «جرائم» يمكن أن تنتهك على الشبكة، وذلك نظراً لمحدودية مستخدميها علاوة على كونها مقصورة على فئة معينة من المستخدمين وهم الباحثين ومنسوبي الجامعات. لهذا فالشبكة ليست آمنة في تصميمها وبناءها. لكن مع توسع استخدام الشبكة ودخول جميع فئات المجتمع إلى قائمة المستخدمين بدأت تظهر جرائم على الشبكة ازدادت مع الوقت وتعددت صورها وأشكالها. والسؤال الذي يطرح نفسه لماذا لا يعاد تصميم الشبكة وبناءها بطريقة تحد من المخاطر الأمنية؟. إن حل جذري كهذا يصعب تنفيذه من الناحية العملية نظرا للتكلفة الهائلة المتوقعة لتنفيذ أي حل في هذا المستوى. إن شبكة الإنترنت كشبكة معلوماتية ينطبق عليها النموذج المعروف لأمن المعلومات ذو الأبعاد الثلاثة وهي:

1 - سرية المعلومات: وذلك يعني ضمان حفظ المعلومات المخزنة في أجهزة الحاسبات أو المنقولة عبر الشبكة وعدم الإطلاع عليها إلا من قبل الأشخاص المخولين بذلك.

2 - سلامة المعلومات: يتمثل ذلك في ضمان عدم تغيير المعلومات المخزنة على أجهزة الحاسب أو المنقولة عبر الشبكة إلا من قبل الأشخاص المخولين بذلك.

3 - وجود المعلومات: وذلك يتمثل في عدم حذف المعلومات المخزنة على أجهزة الحاسب إلا من قبل الأشخاص المخولين بذلك.

إن جرائم الإنترنت ليست محصورة في هذه الجرائم، بل ظهرت جرائم لها صور أخرى متعددة تختلف باختلاف الهدف المباشر في الجريمة. إن أهم الأهداف المقصودة في تلك الجرائم هي كالتالي:

1 - المعلومات: يشمل ذلك سرقة أو تغيير أو حذف المعلومات، ويرتبط هذا الهدف بشكل مباشر بالنموذج الذي سبق ذكره.

2 - الأجهزة: ويشمل ذلك تعطيلها أو تخريبها.

3 - الأشخاص أو الجهات: تهدف فئة كبيرة من الجرائم على شبكة الإنترنت أشخاص أو جهات بشكل مباشر كالتهديد أو الابتزاز.

علماً بأن الجرائم التي تكون أهدافها المباشرة هي المعلومات أو الأجهزة تهدف بشكل غير مباشر إلى الأشخاص المعنيين أو الجهات المعنية بتلك المعلومات أو الأجهزة. بقي أن نذكر أن هناك جرائم متعلقة بالإنترنت تشترك في طبيعتها مع جرائم التخريب أو السرقة التقليدية، كأن يقوم المجرمون بسرقة أجهزة الحاسب المرتبطة بالإنترنت أو تدميرها مباشرة أو تدمير وسائل الاتصال كالأسلاك والأطباق الفضائية وغيرها [1]. حيث يستخدم المجرمون أسلحةً تقليديةً ابتداء من المشارط والسكاكين وحتى عبوات متفجرة، وكمثال لهذا الصنف من الجرائم قام مشغل أجهزة في إحدى الشركات الأمريكية بصب بنزين على أجهزة شركة منافسة وذلك لإحراقها حيث دمر مركز الحاسب الآلي الخاص بتلك الشركة المنافسة برمته. وفيما يلي استعراض لعدد من جرائم الإنترنت:

أولاً: صناعة ونشر الفيروسات: وهي أكثر جرائم الإنترنت انتشاراً وتأثيراً. إن الفيروسات كما هو معلوم ليست وليدة الإنترنت فقد أشار إلى مفهوم فيروس الحاسب العالم الرياضي المعروف فون نيومن في منتصف الأربعينات الميلادية. لم تكن الإنترنت الوسيلة الأكثر استخداما في نشر وتوزيع الفيروسات إلا في السنوات الخمس الأخيرة، حيث أصبحت الإنترنت وسيلة فعالة وسريعة في نشر الفيروسات. ولا يخفى على الكثير سرعة توغل ما يسمى بـ «الدودة الحمراء» حيث استطاعت خلال أقل من تسع ساعات

(1) حجازي، سهير، التهديدات الإجرامية للتجارة الإلكترونية، مركز البحوث والدراسات، شرطة دبي بدولة الإمارات العربية المتحدة، 2005م.

اقتحام ما يقرب من ربع مليون جهاز في 19 يوليو 2001م [1]. إن الهدف المباشر للفيروسات هي المعلومات المخزنة على الأجهزة المقتحمة حيث تقوم بتغييرها أو حذفها أو سرقتها ونقلها إلى أجهزة أخرى.

ثانياً: الاختراقات: تتمثل في الدخول غير المصرح به إلى أجهزة أو شبكات حاسب آلي. إن جل عمليات الاختراقات تتم من خلال برامج متوفرة على الإنترنت يمكن لمن له خبرات تقنية متواضعة أن يستخدمها لشن هجماته على أجهزة الغير، وهنا تكمن الخطورة. تختلف الأهداف المباشرة للاختراقات، فقد تكون المعلومات هي الهدف المباشر حيث يسعى المخترق لتغيير أو سرقة أو إزالة معلومات معينة. وقد يكون الجهاز هو الهدف المباشر بغض النظر عن المعلومات المخزنة عليه، كأن يقوم المخترق للشبكة، هو بقصد إبراز قدراته «الإختراقيه» أو لإثبات وجود ثغرات في الجهاز المخترق. من أكثر الأجهزة المستهدفة في هذا النوع من الجرائم هي تلك التي تستضيف المواقع على الإنترنت، حيث يتم تحريف المعلومات الموجودة على الموقع أو ما يسمى بتغيير وجه الموقع. إن استهداف هذا النوع من الأجهزة يعود إلى عدة أسباب من أهمها كثرة وجود هذه الأجهزة على الشبكة، وسرعة انتشار الخبر حول اختراق ذلك الجهاز خاصة إذا كان يضم مواقع معروفة.

ثالثاً: تعطيل الأجهزة: كثر مؤخراً ارتكاب مثل هذه العمليات[2]، حيث يقوم مرتكبوها بتعطيل أجهزة أو شبكات عن تأدية عملها بدون أن تتم عملية اختراق فعلية لتلك الأجهزة. تتم عملية التعطيل بإرسال عدد هائل من الرسائل بطرق فنية معينة إلى الأجهزة أو الشبكات المراد تعطيلها الأمر الذي يعيقها عن تأدية عملها.

---

(1) Spreutels (J. P.): Les crimes informatiques ET d' autres crimes dans le domaine de la technologie informatique en Belgique, Rev. Int. dr. pen. 1993. p 161.

(2) Fighting Computer Crime: A New Framework for Protecting Information, by Donn B. Parker, 1 edition, John Wiley & Sons 1998.



الفصل الرابع

إجراءات نظر الجرائم المعلوماتية

أمام المحاكم الرقمية

المبحث الأوّل

تحريك الدعوى الجنائية في القانون المصري بوجهٍ عام

الأصل أن: حق تحريك الدعوى الجنائية للنيابة العامة

الجهات الأخرى التي لها حق تحريك الدعوى الجنائية:

ولكن هناك آخرين لهم حق تحريك الدعوى الجنائية وفقاً للقانون وحسب الأحوال التي نذكرها في العناصر الآتية:

المطلب الأول

التصدي

الفرع الأول

مفهوم التصدي

وهو تصدي محكمتي الجنايات والنقض لتحريك الدعوى الجنائية.

علة تقرير حق التصدي:

التقيُّد بشخصية الدعوى الجنائية يعني أن المحكمة الجنائية مقيدة بشخص المتهم المحال إليها في الدعوى فلا تملك المحكمة إلا أن تحكم ببراءته أو بإدانته دون أن تُضيف إليه تهمه أخرى أو أن تُضيف إلى القضية متهمين آخرين، ولكن ما الحل لو وجدت المحكمة أن هناك متهمين آخرين كان يتعين إحالتهم إليها هنا قرر المشرِّع حق التصدي.

ولكن من له حق التصدي؟

قصر المشرِّع حق التصدي على: [1]

1 - محاكم الجنايات: عند نظرها لدعوى مرفوعة أمامها.

2 - الدائرة الجنائية بمحكمة النقض: عند نظر الموضوع بناء على الطعن.

---

(1) حسني، محمود نجيب، شرح قانون الإجراءات الجنائية، الطبعة الثالثة، دار النهضة العربية، القاهرة.

الفرع الثاني
حالات التصدي

الأولى: وجود متهمين آخرين غير مَن أقيمت الدعوى عليهم وكان ينبغي تحريك الدعوى ضدهم سواء بوصفهم فاعلين أصليين للجريمة أم مجرد شركاء فيها.

الثانية: وجود وقائع أخرى ارتكبها المتهم أو المتهمون المقدمون أمامها سواء أكانت جنايات أم جنح.

الثالثة: وجود جناية أو جنحة مرتبطة بالواقعة المطروحة أمام المحكمة ولو كانت قد وقعت من متهمين آخرين غير المقدمين إليها.

الرابعة: وقوع أفعال خارج الجلسة كجريمة مساعدة المقبوض عليه على الفرار وجريمة التوسط لدى قاضٍ، وجريمة التأثير في القضاء بطريق النشر[1].

الفرع الثالث
شروط التصدي

1 - أن تكون هناك دعوى جنائية منظورة أمام محكمة الجنايات أو محكمة النقض.

2 - أن تكون المحكمة قد استظهرت المتهمين الجدد أو الوقائع الجديدة من أوراق الدعوى المعروضة عليها.

3 - ألا تكون الواقعة الجديدة قد أقيمت عنها الدعوى أو مقيدة بقيد

---

(1) عبد الخالق، حسن، أصول الإجراءات الجنائية، الطبعة الثانية عشر، عام 2005م، دار الطبجي للطباعة والنشر، بالقاهرة.

من القيود التي تحول دون تحريكها ومازال القيد قائماً.

4 - أما بالنسبة لمحكمة النقض فيجب أن يكون التصدي أثناء نظرها للموضوع للطعن بالنقض للمرة الثانية فلا يجوز لها مباشرة حق التصدي في حالة الطعن بالنقض للمرة الأولى.

5 - أن تكون المحكمة المتصدية بصدد حالة من الحالات التي أجاز فيها القانون التصدي.

الفرع الرابع
إجراءات وآثار التصدي

إجراءات التصدي:

إذا توافرت شروط التصدي فإنه يجوز للمحكمة إصدار قرار تتخذ به أحد أمرين:

أولهما: إحالة الدعوى الجديدة إلى النيابة العامة لتحقيقها والتصرف فيها.

ثانيهما: انتداب أحد أعضاء المحكمة للقيام بإجراءات التحقيق.

آثار التصدي:

يقتصر أثر التصدي على إحالة الدعوى الجنائية على النيابة العامة أو ندب أحد أعضائها للتحقيق دون أن تكون ملتزمة برفع الدعوى إلى المحكمة فيجوز لها ما يجوز للنيابة العامة وذلك من النظام العام ولذلك يترتب على مخالفتها البطلان المطلق.

سلطة المحاكم في تحريك الدعوى في جرائم الجلسات:

أولاً: بيان الاستثناء:

يُقصد بجرائم الجلسات تلك الجرائم التي تقع أثناء انعقاد جلسات المحكمة.

ثانياً: ضبط الجلسة وإدارتها:

ضبط الجلسة وإدارتها منوطان برئيسها وله في سبيل ذلك أن يُخرج من قاعة الجلسة مَن يخل بنظامها فإن لم يمتثل وتمادى كان للمحكمة أن تحكم على الفور بحبسه أربعاً وعشرين ساعة أو بتغريمه عشرة جنيهات ويكون حكمها نهائي.

المطلب الثاني

نطاق تحريك الدعوى في جرائم الجلسات

أولاً: جرائم جلسات المحاكم الجنائية:

إذ وقعت جنحة أو مخالفة في الجلسة يجوز للمحكمة أن تُقيم الدعوى على المتهم في الحال وتحكم عليه بعد سماع أقوال النيابة العامة ودفاع المتهم إلا في حالة ارتكاب جناية فإن صلاحيات المحكمة تقتصر على إحالة المتهم إلى النيابة العامة دون أن يكون لها إجراء تحقيق للدعوى ويكون الطعن في الأحكام الصادرة في جرائم الجلسات وفقاً للقواعد العامة[1].

ثانياً: جرائم جلسات المحاكم المدنية:

للمحكمة أن تُحاكم مَن تقع منه أثناء انعقادها جنحة تعد على هيئتها أو على أحد أعضائها أو أحد العاملين بالمحكمة وتحكم عليه فوراً بالعقوبة وأن تُحاكم مَن شهد زوراً بالجلسة وتحكم عليه ويكون حكم المحكمة في هذه الأحوال نافذاً ولو حصل استئنافه.

---

(1) عبد الخالق، حسن، أصول الإجراءات الجنائية، المرجع السابق.

ثالثاً: جرائم المحامين في جلسات المحاكم:

إذا وقع من المحامي أثناء وجوده بالجلسة لأداء واجبه أو بسببه إخلال بنظام الجلسة أو أي أمر يستدعي محاسبته نقابياً أو جنائياً يأمر رئيس الجلسة بتحرير مذكرة بما حدث ويُحيلها إلى النيابة العامة ويخطر النقابة الفرعية بذلك يجوز القبض على المحامي أو حبسه احتياطياً ولا ترفع الدعوى الجنائية فيها إلا بأمر من النائب العام أو مَن ينوب عنه من المحامين العامين الأول[1].

طالع أيضاً: النائب العام المصري، النيابة العامة ودعواه اتخاذ أول إجراء من إجراءاتها، وبتعبير آخر هو: الإجراء الذي ينقل الدعوى من حال السكون التي كانت عليه عند نشأتها إلى حال الحركة بأن يدخلها في حوزة السلطات المختصة باتخاذ الإجراءات التالية.

وأهم أمثلة إجراءات تحريك الدعوى:

1 - انتداب النيابة العامة مأمور الضبط القضائي لإجراء عمل من أعمال التحقيق.

2 - قرار النيابة العامة تولي التحقيق بنفسها، وتكليفها المتهم بالحضور أمام محكمة الجنح والمخالفات.

3 - إقامة المدعية بالحقوق المدنية دعواه أمام المحكمة الجنائية التي ينبني عليها.

ومن المعلوم أن النظم التشريعية في تحريك الدعوى الجنائية واستعمالها تنقسم إلى نظامين، أولهما حتمية تحريك الدعوى الجنائية واستعمالها على أساس إلزام النيابة العامة بتحريك الدعوى الجنائية واستعمالها إذا توافرت أركان الجريمة، وثانيهما، ملائمة تحريكها واستعمالها، على أساس من إعطاء النيابة العامة سلطة تقديرية في ذلك، فيكون لها أن تمتنع عن تحريك الدعوى واستعمالها على الرغم ن توافر جميع أركان الجريمة إذا قدّرت أن المصلحة

(1) حسني، محمود نجيب، شرح قانون الإجراءات الجنائية، المرجع السابق.

العامة تقتضي ذلك. هذا وقد تبنى المشرِّع المصري النظامين معاً، فقد ميّز بين مرحلتين للدعوى؛ تحريكها، واستعمالها. فأخذ ناحية، الملائمة بالنسبة لتحريكه، وأقرّ مبدأ الحتمية بالنسبة لاستعمالها. فمن ناحية، لم يطلق سلطة النيابة العامة في تحريكها، ومن ناحية أخرى لم يتقبل احتكار النيابة العامة تحريك الدعوى الجنائية [1].

فاختصاص النيابة العامة بتحريك الدعوى الجنائية هي الأصل والاستثناء في شكل تحفظين. أنه ثمة قيود تؤثر على سلطة النيابة العامة في تحريك الدعوى الجنائية. ووجود أشخاص تشارك النيابة العامة سلطة تحريك الدعوى الجنائية[2].

المطلب الثالث

الشكوى

الفرع الأول

مفهوم الشكوى وحالاتها

الشكوى باعتبارها قيداً على سلطة النيابة في تحريك الدعوى الجنائية:

أولاً: تعريف الشكوى:

الشكوى هي تعبير غير مقيد يصدر من المجني عليه أو ممّن يُمثّله يوجه إلى النيابة العامة أو إلى أحد مأموري الضبط القضائي ويكشف بوضوح عن

(1) حسني، محمود نجيب، شرح قانون الإجراءات الجنائية، المرجع السابق.

(2) الزهني، لأدور غالي، الاجرءات الجنائية، الطبعة الثالثة، مكتبة غريب بالقاهرة، 1990م

إرادة المجني عليه في تحريك الدعوى الجنائية ضد المتهم [1].

ثانياً: حالات الشكوى:

لا يجوز أن ترفع الدعوى إلا بناء على شكوى شفهية أو كتابية من التالية: في الجرائم التالية:

1 - جريمة زنا الزوجة أو زنا الزوج.

2 - جريمة ارتكاب أمر مخل بالحياء مع امرأة ولو في غير علانية.

3 - جريمة امتناع الوالدين أو الجدين عن تسليم الصغير لمن له الحق في طلبه بناء على قرار من جهة القضاء صادر بشأن حضانته أو خطفه.

4 - جريمة الامتناع عن دفع النفقة أو أجرة الحضانة أو الرضاعة أو السكن الصادر بها حكم قضائي واجب النفاذ.

5 - جرائم السب والقذف.

6 - جريمة السرقة إضرار بالزوج أو الأصول أو الفروع.

7 - جريمة مروق الحدث من سلطة ولى الأمر.

الفرع الثاني

علة تقرير قيد الشكوى

قد يرى المجني عليه أن الأضرار التي تقع عليه من جراء محاكمة الجاني أشد ضرراً من الضرر الناشئ عن ارتكاب الجريمة ذاتها. لما في إجراءات المحاكمة من العلانية لا تُصيب الجاني وحده وإنما قد يمتد أثرها

(1) عبد الخالق، حسن، أصول الإجراءات الجنائية، المرجع السابق.

إلى المجني عليه نفسه[1].

الفرع الثالث

ممن تقدم القيم

تقدم الشكوى من المجني عليه بشخصه أو ممَّن يُمثِّله مثل:

1 - الولي: إذا كان المجني عليه دون الخامسة عشر من عمره.

2 - الوصي أو القيم: إذا كانت الجريمة واقعة على المال.

3 - النيابة العامة: إذا تعارضت مصلحة المجني عليه مع مصلحة من يُمثله وإذا كانت النيابة اتفاقية فيشترط أن يكون التوكيل خاصاً وصريحاً وصادراً، وإذا تعدد المجني عليهم أن تقدم الشكوى من أحدهم وينقضي الحق في الشكوى من أحدهم وينقضي الحق في الشكوى بوفاة المجني عليه، ويجب أن يكون الشاكي متمتعاً بأهلية الشكوى، وهو يكون كذلك إذا بلغ من العمر خمسة عشر عاماً[2].

الفرع الرابع

ضد من تقدم الشكوى؟

تقدم الشكوى ضد المسئول جنائياً عن الجريمة فاعلاً كان أم شريكاً

---

(1) حسني، محمود نجيب، شرح قانون الإجراءات الجنائية، المرجع السابق.

(2) الزهني، لأنور غالي، الاجرءات الجنائية، المرجع السابق.

،ويجب أن يتم تعيينه كافياً فلا عبرة بالشكوى إذا قدمت ضد مجهول وإذا تعدد المتهمون فيكفي أن تقدم الشكوى ضد أحدهم والنيابة العامة تملك تحريك الدعوى ضد الباقين باستثناء جريمة الزنا[1].

إلى مَن تُقدم الشكوى؟

تُقدم الشكوى إلى النيابة العامة أو إلى مأموري الضبط القضائي أو على مَن يكون حاضراً من رجال السلطة العامة في حالة التلبس بارتكاب الجريمة، ويُعتبر تحريك الدعوى الجنائية بطريق الادعاء المباشر بمثابة شكوى.

متى تُقدم الشكوى؟

تُقدم الشكوى خلال ثلاثة أشهر تبدأ من يوم علم المجني عليه بالجريمة وبمرتكبها.

شكل الشكوى:

لم يشترط القانون في الشكوى شكلاً معيناً فقد أجاز أن تُقدم شفاهه أو كتابة وغير معلقة وتُعتبر شكوى استغاثة المجني عليه من الجاني لمن يكون حاضراً من رجال السلطة العامة [2].

الفرع الخامس

الشكوى والارتباط بين الجرائم

1 - حالة التعدد المعنوي أو الصوري أو الظاهري: إذا كون الفعل

(1) عبد الخالق، حسن، أصول الإجراءات الجنائية، المرجع السابق.

(2) حسني، محمود نجيب، شرح قانون الإجراءات الجنائية، المرجع السابق.

الواحد جرائم متعددة وجب اعتبار الجريمة التي عقوبتها أشد والحكم بها دون غيرها، فإذا ارتكبت الزوجة جريمة الزنا في مكان عام فيكون لهذا الفعل وصفان جريمة الزنا وجريمة الفعل الفاضح ولما كانت جريمة الزنا هي الجريمة التي عقوبتها أشد وحيث أن القانون استلزم الشكوى في جريمة الزنا؛ لذلك فإنه يمتنع على النيابة تحريك الدعوى عن الفعل الإجرامي سواء بالوصف الأشد أو بالوصف الأخف.

2 - حالة التعدد المادي أو الحقيقي أو الفعلي: في هذه الحالة نكون أمام أفعال إجرامية متعددة بحيث يُشكل كل فعل منها جريمة مستقلة، فلو قام شخص بضرب وسب آخر في هذه الحالة يجوز للنيابة العامة تحريك الدعوى الجنائية عن جريمة الضرب وتمتنع عن تحريك الدعوى بالنسبة لجريمة السب التي تلزم فيها الشكوى[1].

الشكوى وحالة التلبس:

إذا كانت الجريمة المتلبس بها مما يتوقف عليها رفع الدعوى العمومية عنها على شكوى فلا يجوز القبض على المتهم إلا إذا صرح بالشكوى مَن يملك تقديمها ويجوز في هذه الحالة أن تكون الشكوى لمن يكون حاضراً من رجال السلطة العامة باستثناء جريمة الزنا.

الفرع السادس

الآثار التي تترتب على تقديم الشكوى

بعد تقديم الشكوى ممَّن يملكها، فإن للنيابة العامة كامل حريتها في القيام بكافة إجراءات التحقيق، ولها كامل صلاحيتها في تقدير مدى ملائمة تحريك الدعوى الجنائية ضد المتهم من عدمه فقد تأمر النيابة بحفظ الشكوى إدارياً[2].

(1) الزهني، لأدور غالي، الاجراءات الجنائية، المرجع السابق.

(2) الزهني، لأدور غالي، الاجراءات الجنائية، المرجع السابق.

الفرع السابع

سقوط وانقضاء الحق في الشكوى والتنازل عنها

سقوط الحق في الشكوى:

الحالة الأولى: سبق ارتكاب الزوج جريمة الزنا:

إذا كان قد سبق للزوج المجني عليه أن ارتكب جريمة الزنا في المسكن المقيم فيه مع زوجته فلا تسمع دعواه عليها والعكس غير صحيح.

الحالة الثانية: رضاء الزوج مقدماً بارتكاب زوجته جريمة الزنا:

إن رضاء الزوج لزوجته ارتكاب جريمة الزنا لا يسقط حقه في الشكوى فإذا ثبت أن الزوج كان يسمح لزوجته بالزنا بل وأنه قد اتخذ الزواج حرفة يبغي من ورائها العيش مما تكسبه زوجته من البغاء، فإن مثل هذا الزوج لا يصح أن يُعتبر زوجاً حقيقة وليس له أن يطلب محاكمة زوجته [1].

انقضاء الحق في الشكوى:

1 - مضي المدة: ينقضي الحق في الشكوى بمضي ثلاثة أشهر من يوم علم المجني عليه بالجريمة وبمرتكبها.

2 - وفاة المجني عليه: الحق في الشكوى من الحقوق اللصيقة بشخصية المجني عليه، فإذا توفي المجني عليه دون تقديمها فلا ينتقل هذا الحق إلى ورثته ولا يحق لأي منهم تقديمها.

التنازل:

- **تعريف التنازل:**

التنازل عن الشكوى هو تعبير يصدر من المجني عليه يكشف عن إرادته

(1) حسني، محمود نجيب، شرح قانون الإجراءات الجنائية، المرجع السابق.

في عدم اتخاذ الإجراءات أو عدم استمرارها.

ممَّن يُقدم التنازل؟

يُقدم التنازل من المجني عليه صاحب الحق في الشكوى ويشترط أن تتوافر لديه أهلية الشكوى، وإذا تطلب القانون صفة خاصة في الشاكي فيجب أن تتوافر هذه الصفة عند تقديم التنازل ولا يُستثنى من ذلك إلا حالة الزنا؛ حيث اشترط القانون توافر صفة الزوج لقيام رابطة الزوجية عند تقديم الشكوى ولم يشترط توافر هذه الصفة عند التنازل عنها وإذا توفي الشاكي فلا ينتقل حقه في التنازل إلى ورثته إلا في دعوى الزنا.

• شكل التنازل:

لم يشترط القانون شكلاً معيناً للتنازل، فيستوي أن يقرُّ به الشاكي كتابة أم شفاهة أو أن يكون صريحاً أم ضمنياً، وقد يُستفاد من تصرف معين كأن يعود الزوج إلى معاشرة زوجته الزانية [1].

لمن يُقدم التنازل؟

لم يشترط القانون تقديم التنازل لجهة معينة فيصح تقديمه إلى النيابة العامة أو إلى أحد مأموري الضبط القضائي كما يصح تقديمه إلى المحكمة.

• وقت التنازل:

أجاز القانون التنازل عن الشكوى في أي وقت إلى أن يصدر في الدعوى حكم نهائي، فتنقضي الدعوى الجنائية بالتنازل وقد استثنى المشرِّع حالتين أجاز فيهما للمجني عليه أن يوقف تنفيذ الحكم الواجب النفاذ وهما [2]:

---

(1) حسني، محمود نجيب، شرح قانون الإجراءات الجنائية، المرجع السابق.

(2) حسني، محمود نجيب، شرح قانون الإجراءات الجنائية، المرجع السابق.

الحالة الأولى: لزوج المرأة الزانية أن يوقف تنفيذ الحكم عليها برضائه معاشرتها له كما كانت.

الحالة الثانية: للمجني عليه في السرقة بين الأزواج والأصول والفروع أن يوقف تنفيذ الحكم النهائي على الجاني في أي وقت شاء.

- **أثر التنازل:**

يترتب على التنازل انقضاء الدعوى الجنائية وللمتهم أن يتمسك بالتنازل في أية حالة كانت عليها الدعوى ولو لأول مرة أمام محكمة النقض؛ لأن انقضاء الدعوى الجنائية من النظام العام ولا يؤثر ذلك على الدعوى المدنية التبعية ولكن يُستثنى من ذلك جريمة الزنا، إذ ينصرف تنازل الزوج المجني عليه عن شكواه إلى الدعوى الجنائية إلى الدعوى المدنية أيضاً[1].

المطلب الثاني

الطلب

الفرع الأول

مفهوم الطلب

الطلب: هو تعبير يصدر من إحدى الهيئات العامة التي عينها القانون يُوجه إلى النيابة العامة ويكشف بوضوح عن إرادة الهيئة العامة في تحريك الدعوى الجنائية ضد المتهم ويترتب على تقديم الطلب إطلاق حرية النيابة العامة في تقدير مدى ملائمة تحريك الدعوى الجنائية من عدمه.

---

(1) عبد الخالق، حسن، أصول الإجراءات الجنائية، المرجع السابق.

الفرع الثاني

أحوال الطلب

1 - جريمة العيب في حق ملك أو رئيس دولة أجنبية.

2 - جريمة العيب في حق ممثل لدولة أجنبية معتمد في مصر بسبب أمور تتعلق بأداء وظيفته.

3 - جرائم إهانة، أو سب مجلس الشعب، أو غيره من الهيئات النظامية، أو الجيش، أو المحاكم، أو السلطات، أو المصالح العامة.

4 - الجرائم الضريبية.

5 - جرائم التهريب الجمركي.

6 - جرائم تهريب النقد الأجنبي.

وقد وردت هذه الحالات على سبيل الحصر وهي تتميز بطابع استثنائي شأنها في ذلك شأن الشكوى؛ ولذلك فلا يجوز القياس عليها [1].

الفرع الثالث

علة تقرير قيد الطلب

قدر المشرِّع أن هناك بعض الجرائم تستوجب أن يكون تقدير مدى

(1) الزهني، لأنور غالي، الاجرءات الجنائية، المرجع السابق.

ملائمة رفع الدعوى فيها من عدمه متروكاً إلى جهات أخرى غير النيابة العامة؛ حيث تكون هذه لجهات بحكم وضعها وظروفها أقدر على فهم كافة الظروف والملابسات ووزن كافة الاعتبارات لتقرير رفع الدعوى الجنائية من عدمه.

الفرع الرابع

تقديم الطلب وشروطه

ممن يقدم الطلب؟

1 – وزير العدل بالنسبة للجريمتين أرقان1.

2 – رؤساء الهيئات المجني عليها بالنسبة للجريمة رقم3.

3 – وزير المالية أو من يندبه بالنسبة لباقي الجرائم.

لمن يُقدم الطلب؟

يُقدم الطلب إلى النيابة العامة بحسبانها الجهة صاحبة الاختصاص الأصيل بتحريك الدعوى النائية.

شروط الطلب:

1 – أن يكون الطلب صادراً ممَّن له سلطة إصداره أصالة أو إنابة.

2 – أن يكون الطلب مكتوباً وموقَّعاً عليه ممَّن أصدره.

3 – أن يكون كاشفاً بوضوح عن إرادة الجهة الرسمية في تحريك الدعوى الجنائية ضد المتهم.

4 – يشترط أن يتضمن الطلب بياناً بالواقعة أو الوقائع المطلوب تحريك الدعوى الجنائية عنها.

5 - وتقديم الطلب غير مقيَّد بوقت معين.

آثار تقديم الطلب:

يترتب على تقديم الطلب ذات الأثر المترتب على تقديم الشكوى؛ حيث تسترد النيابة العامة حريتها في تقدير مدى ملائمة تحريك الدعوى، أو الأمر بحفظ الأوراق، أو بالأوجه لإقامة الدعوى.

التنازل عن الطلب:

للجهة التي قدَّمت الطلب حق التنازل عنه كتاباً في أية حالة كانت عليها الدعوى حتى صدور حكم بات فيها وبتقديم التنازل تنقضي الدعوى.

المطلب الثالث

الإذن

الفرع الأول

مفهوم الإذن

استوجب القانون في أحوال معينة الحصول على إذن من الهيئة التي ينتمي إليها المتهم كشرط لإمكان تحريك الدعوى الجنائية ضده رعاية للوظيفة التي يشغلها، فقد يترتب على رفع الدعوى مساس بالاستقلال الذي ينبغي أن يتوفر لهم لأداء الواجبات المنوطة بهم.

أولاً: الحصانة البرلمانية أو النيابية: الحصانة البرلمانية تخضع للقواعد الآتية:

1 - إن الحصانة لا تسري إلا على مَن يتمتع بصفة العضو في مجلس الشعب.

2 - الحصانة تشمل جميع الجرائم دون تحديد.

3 - أن نطاق الحصانة يقتصر على الإجراءات الجنائية فحسب.

4 – أن سريان الحصانة على عضو مجلس الشعب يظل مستمراً منذ بداية عضويته في المجلس وحتى انتهاء مدة العضوية.

5 – أن الحصانة لا تشمل حالة التلبس بالجريمة.

6 – أن الإذن يصدر من مجلس الشعب فإذا كان المجلس في غير دور انعقاد يتعين صدوره من رئيس المجلس.

7. أن النظر في إصدار الإذن يكون بناء على طلب من النيابة العامة أو من المحكمة[1].

ثانياً، الحصانة القضائية: تخضع الحصانة القضائية للقواعد الآتية:

1 – أن الحصانة القضائية تنصرف إلى القضاة على اختلاف مسمياتها الوظيفية، وأعضاء النيابة العامة، وأعضاء مجلس الدولة، وأعضاء هيئة قضايا الدولة والحصانة تلازم التمتع بالصفة القضائية وتدور معها وجوداً وعدماً.

2 – أن هذه الحصانة تقتصر على الجنايات والجنح دون المخالفات لبساطتها.

3 – والإذن شخصي بحت فمتى صدر الإذن عن شخص معين فلا ينصرف إلا إليه.

4 – أن هذه الحصانة تنحسر عن القاضي في حالة تلبسه بارتكاب الجناية أو الجنحة.

5 – في غير حالات التلبس فلا يجوز اتخاذ أية إجراءات جنائية ماسة بشخص القاضي قبل صدور الإذن من اللجنة المختصة ويقع باطلاً كل إجراء يخالف ذلك [2].

---

(1) عبد الخالق، حسن، أصول الإجراءات الجنائية، المرجع السابق.

(2) سلامة، مأمون، الإجراءات الجنائية في القانون المصري، ج 2، ط2000م، منشورات المكتبة

المطلب الرابع

انقضاء الدعوى في القانون المصري (1)

الفرع الأول

وفاة المتهم

أولاً: وفاة المتهم قبل تحريك الدعوى الجنائية:

إذا حصلت الوفاة قبل تحريك الدعوى الجنائية فلا يجوز تحريكها وتصدر النيابة العامة أمراً بحفظ الأوراق.

ثانياً: إذا حصلت الوفاة أثناء الدعوى:

فتقضي المحكمة بسقوط الدعوى الجنائية ويمتنع عليها أن تقضي بأية عقوبة.

ثالثاً: وفاة المتهم بعد صدور حكم غير بات:

إذا حدثت الوفاة بعد صدور الحكم وقبل الفصل في الطعن فإن الحكم يُمحى بسقوط الدعوى، وفي هذه الحالة يجب رد العقوبات المالية التي تم تنفيذها فيرد مبلغ الغرامة والأشياء التي صودرت.

رابعاً: وفاة المتهم بعد صدور حكم بات:

إذا حدثت الوفاة بعد صدور حكم بات، فإنه يترتب على الوفاة سقوط العقوبة المقضي بها.

خامساً: ظهور المتهم حياً بعد الحكم بانقضاء الدعوى الجنائية لوفاته:

إذا قضت المحكمة بانقضاء الدعوى الجنائية لوفاة المتهم، ثم تبين بعد

الجامعة.

(1) الزهني، لأدور غالي، الاجراءات الجنائية، المرجع السابق.

ذلك أنه لا يزال على قيد الحياة فإن هذا الحكم لا يُعد فاصلاً في موضوع الدعوى الجنائية، ومن ثم فلا يحوز حجية الشيء المقضي فيه.

سادساً: استمرار نظر المحكمة للدعوى الجنائية لجهلها بوفاة المتهم:

إذا استمرت المحكمة في نظر الدعوى الجنائية وأصدرت فيها حكماً غيابياً في حين أن المتهم قد توفي قبل إصدار الحكم ولم تكن المحكمة على علم بوفاته، فإن الحكم الذي يصدر في هذه الحالة يكون منعدماً لعدم قيام الدعوى وقت إصداره وذلك لانقضائها قانوناً بوفاة المتهم [1].

سابعاً: أثر وفاة المتهم على الدعوى المدنية:

لا أثر لوفاة المتهم على الدعوى المدنية المترتبة على الجريمة وتظل قائمة وحدها أمام القضاء الجنائي مادامت قد رفعت مع الدعوى الجنائية

ثامناً: أثر وفاة المتهم على المساهمين الآخرين في ارتكاب الجريمة:

إذا توفي المتهم سواء كان فاعلاً أصلياً أم شريكاً في الجريمة، فإنه يترتب على وفاته انقضاء الدعوى الجنائية بالنسبة له ولا أثر لوفاته على بقية المساهمين الآخرين معه في ارتكاب الجريمة [2].

الفرع الثاني
العفو الشامل

النوع الأول: العفو عن العقوبة:

وهي صلاحية مخولة لرئيس الجمهورية يكون له بمقتضاها حق إسقاط العقوبة كلها، أو بعضها، أو إبدالها بعقوبة أخف منها مقررة قانوناً، ولا تسقط

(1) سلامة، مأمون، الاجراءات الجنائية في القانون المصري، المرجع السابق.
(2) حسني، محمود نجيب، شرح قانون الإجراءات الجنائية، المرجع السابق.

العقوبة التبعية ولا الآثار الجنائية الأخرى المترتبة على الحكم بالإدانة ما لم ينص في أمر العفو على خلاف ذلك.

النوع الثاني: العفو عن الجريمة:

العفو عن الجريمة، أو العفو الشامل، أو العام يعني تجريد الفعل من الصفة الإجرامية، فيصبح كما لو كان فعلاً مباحاً وهو حق مقرر للهيئة الاجتماعية؛ ولذلك فلا يكون إلا بقانون.

الفرع الثالث

مضي المدة

أولاً: مبدأ التقادم وتبريره:

يرتب القانون على مضي مدة معينة على ارتكاب الجريمة دون اتخاذ إجراءات فيها سقوط الدعوى الجنائية بالتقادم؛ لأن مضي مدة معينة على ارتكاب الجريمة يؤدي إلى نسينها [1].

ثانياً: مدة التقادم:

تنقضي الدعوى الجنائية بالتقادم في مواد الجنايات بمضي عشر سنين وفي مواد الجنح بمضي ثلاث سنين وفي مواد المخالفات بمضي سنة.

ثالثاً: نطاق التقادم:

استثنى المشرّع الجرائم الآتية:

1 - جريمة تعذيب المتهم لحمله على الاعتراف.

(1) حسني، محمود نجيب، شرح قانون الإجراءات الجنائية، المرجع السابق.

2 - جريمة معاقبة المحكوم عليه بعقوبة لم يحكم عليها بها.

3 - جريمة القبض بغير وجه حق من شخص تزيا بدون وجه حق بزي مستخدمي الحكومة.

4 - جرائم الاعتداء على حرمة الحياة الخاصة للمواطن [1].

رابعاً: بدء سريان مدة التقادم:

الأصل أن تبدأ مدة التقادم من اليوم التالي لوقوع الجريمة ويُستثنى جرائم اختلاس المال العام والعدوان عليه والغدر ولا تستكمل المدة إلا بانقضاء اليوم الأخير ويختلف ميعاد بدء سريان التقادم باختلاف نوع الجريمة وطبيعتها على التفصيل الآتي:

1 - الجرائم الوقتية الأفعال: التقادم من اليوم التالي لتاريخ وقوعها.

2 - الجرائم المستمرة: تبدأ مدة التقادم من اليوم الذي ينتهي فيه النشاط الإجرامي المكون لحالة الاستمرار.

3 - الجرائم متتابعة الأفعال: كجريمة سرقة التيار الكهربائي فإن مدة التقادم تبدأ من اليوم التالي لتاريخ ارتكاب آخر فعل من أفعال التتابع.

4 - سادسا: العادة: وهي الجرائم التي لا تقوم إلا بتكرار فعل واحد أكثر من مرة كجريمة الاعتياد على الإقراض بالربا الفاحش، فإن مدة التقادم تبدأ من يوم تمام تكوين الجريمة [2].

خامساً: وقف مدة التقادم:

يُقصد بوقف التقادم قيام مانع يؤدي على وقف سريان مدة التقادم

(1) سلامة، مأمون، الإجراءات الجنائية في القانون المصري، المرجع السابق.

(2) عبد الخالق، حسن، أصول الإجراءات الجنائية، المرجع السابق.

حتى زوال هذا المانع ثم استئناف سريان التقادم استكمالاً للمدة التي انقضت قبل قيام مانع وقد حسم المشرِّع الأمر بنصه لا يوقف سريان المدة التي تسقط بها الدعوى الجنائية لأي سبب كان باستثناء جرائم اختلاس الأموال الأميرية والغدر.

سادساً: انقطاع مدة التقادم:

انقطاع مدة التقادم يعني سقوط المدة التي انقضت منه وبدء سريان مدة جديدة وذلك نتيجة إجراء من إجراءات الدعوى الجنائية التي حدَّدها القانون على سبيل الحصر.

سابعاً: مالا يقطع مدة التقادم:

لا يقطع مدة التقادم أي إجراء من الإجراءات التي عن نطاق الدعوى الجنائية كالإبلاغ عن الجريمة.

ثامناً: شروط الإجراء القاطع لمدة التقادم:

يشترط في الإجراء القاطع للتقادم أن يكون صحيحاً مستوفياً لكافة الشرائط الشكلية والموضوعية التي عيناها القانون حتى يرتب أثره بقطع مدة التقادم وعلى ذلك فلا ينقطع التقادم بالتحقيق الذي يجاوز حدود الاختصاص لمن باشره.

الفرع الرابع

الحكم البات

الحكم البات هو السبب الطبيعي لانقضاء الدعوى الجنائية فتنقضي الدعوى الجنائية بالنسبة للمتهم المرفوعة عليه والوقائع المسندة فيها إليه بصدور حكم نهائي فيها بالبراءة أو الإدانة حتى ولو بناء على ظهور أدلة جديدة تغيير الوصف القانوني للجريمة.

المبحث الثاني

تحريك الدعاوى في النظام الجزائي السعودي

المطلب الأول

جمع الاستدلالات

الفرع الأول

مفهوم جمع الاستدلالات والسلطة المختصة به

أولاً: مفهوم جمع الاستدلالات:

يُقصد بجمع الاستدلالات جميع الإجراءات التي يُباشرها رجال الضبط الجنائي للتحري عن الجريمة والبحث عن مرتكبيها، وجمع كافة البيانات عن زمان ومكان ارتكابها، وأشخاصها أو مَن يحتمل مساهمتهم في ارتكابها، وشهودها، وبالجملة كافة المعلومات التي يمكن أن تؤدي إلى كشف الجريمة أو تحديد شخصية مرتكبيها، ووضع المعلومات المذكورة بين يدي سلطة التحقيق، وتبدأ مرحلة جمع الاستدلالات من لحظة وقوع الجريمة وتنتهي بتقديم المحضر المتضمن كافة البيانات إلى هيئة التحقيق [1] وعرف مشروع اللائحة التنفيذية لنظام الإجراءات الجزائية جمع الاستدلال بأنه: «السعي لإظهار الحقيقة عن طريق جمع عناصر الإثبات الخاصة بالجريمة، والتحري عنها، والبحث عن فاعليها، والإعداد للبدء في التحقيق أو المحاكمة مباشرة».

(1) عبد الخالق، حسن، أصول الإجراءات الجنائية، المرجع السابق.

ثانياً: السلطة المختصة بجمع الاستدلالات:

نصت المادة 24 جزائية على أن: «رجال الضبط الجنائي هم الأشخاص الذين يقومون بالبحث عن مرتكبي الجرائم وضبطهم وجمع المعلومات والأدلة اللازمة للتحقيق وتوجيه الاتهام»، طبقاً لذلك فإن رجال الضبط الجنائي هم المختصين نظامياً بجمع الاستدلالات والقيام بالتحريات اللازمة لجمع الأدلة التي تُفيد في كشف الحقيقة.

الفرع الثاني

الضبط الجنائي

إجراءات الضبط الجنائي هي إجراءات جمع الاستدلال التي تعقب وقوع جريمة وتسبق مرحلة التحقيق فيها، ولا تكون إلا بصدد جريمة فلا تُتخذ إلا بصدد فعل محظور ومعاقب عليه شرعاً أو نظاماً، فكل واقعة لا ينطبق عليها وصف الجريمة لا تباشر حيالها إجراءات الضبط الجنائي ولو ترتب عليها ضرر.

أولاً: فرق بين الضبط الجنائي والضبط الإداري:

الضبط الإداري يُقصد به مجموع الإجراءات والأوامر والقرارات التي تتخذها السلطة المختصة بالضبط من أجل المحافظة على النظام العام في المجتمع فهي مجموعة الإجراءات المقررة السابقة على وقوع الجريمة لمنع ارتكابها فإذا وقت الجريمة تبدأ مرحله الضبط الجنائي، فالضبط الإداري سابق على ارتكاب مخالفات النظام العام، فهو يستهدف تفادي كل ما يؤدي إلى الإخلال بالنظام العام، وذلك بإصدار الأوامر والنواهي التي تحول دون الإخلال بالنظام العام بعناصره الثلاثة (الأمن العام - الصحة العامة -

السكينة العامة)، بينما مهمة رجل الضبط الجنائي تبدأ بعد عجز رجل الضبط الإداري عن الحيلولة دون وقوع الجريمة ويقصد بها جميع الإجراءات التي يُباشرها رجال الضبط الجنائي للتحري عن الجريمة والبحث عن مرتكبيها.

ثانياً: سلطات وواجبات رجال الضبط الجنائي في مرحلة جمع الاستدلالات:

نصت المادة 27 جزائية على أن: «على رجال الضبط الجنائي كل حسب اختصاصه أن يقبلوا البلاغات والشكاوى التي ترد إليهم في جميع الجرائم، وأن يقوموا بفحصها وجمع المعلومات المتعلّقة بها في محضر موقع عليه منهم، وتسجيل ملخصها وتاريخها في سجل يُعد لذلك، مع إبلاغ هيئة التحقيق والادعاء العام بذلك فوراً. ويجب أن ينتقل رجل الضبط الجنائي بنفسه إلى محل الجرائم، محافظة عليه، وضبط كل ما يتعلّق بالجريمة، والمحافظة على أدلتها، والقيام بالإجراءات التي تقتضيها الحال، وعليه أن يثبت جميع هذه الإجراءات الخاصة بذلك وبمقتضى ذلك النص يمكن تحديد اختصاصات رجال الضبط الجنائي في مرحلة الاستدلالات على النحو الآتي:

1 - قبول البلاغات والشكاوى التي ترد إليهم في جميع الجرائم، وفحصها، وجمع المعلومات المتعلّقة بها، أيّاً كانت وسيلة علمهم بها، ما دامت الوسيلة مشروعة.

2 - الحصول على المتهم. ت اللازمة ممن لديهم معلومات عن الواقعة الجنائية ومرتكبها؛ كالمبلغ، والمشتبه فيه، والشهود وغيرهم، وهذه الإيضاحات تختلف عن الاستجواب؛ لأن الاستجواب يُقصد به مناقشه المتهم تفصيلاً في التهمه المنسوبة إليه والأدلة.

3 - سماع أقوال المتهم، والتحري عنه بجمع المعلومات المختلفة التي تبيّن شخصيته.

4 - الانتقال إلى محل الحادث للمحافظة عليه وضبط كل ما يتعلّق بالجريمة والمحافظة على أدلتها؛ وذلك بالتحفظ على مكان الجريمة بإبعاد الأشخاص الموجودين به دون داعٍ، ومنع اقتراب أحد منه أو العبث بمحتوياته لمحافظته عليه.

5 - إبلاغ هيئة التحقيق والادعاء العام بذلك.

6 - إثبات جميع هذه الإجراءات في المحضر الخاص بذلك، يُسمى محضر جمع الاستدلال.

مع ملاحظة وجود بعض السلطات الأخرى الاستثنائية لرجال الضبط الجنائي مثل القبض والتفتيش وفى أحوال معينة كالتلبس وسنوضحها تباعاً حين التعرُّض لها.

ثالثاً: الأشخاص المسند إليهم مهمة الضبط الجنائية:

حدَّد نظام الإجراءات الجزائية رجال الضبط الجنائي حسب المهام الموكولة إليهم، وأوردهم على سبيل الحصر في المادة السادسة والعشرين من النظام، حيث نصت على أن: يقوم بأعمال الضبط الجنائي، حسب المهام الموكولة إليه، كل من:

1 - أعضاء هيئة التحقيق والادعاء العام في مجال اختصاصهم.

2 - مديري الشرط ومعاونيهم في المناطق والمحافظات والمراكز.

3 - ضباط الأمن العام، وضباط المباحث العامة، وضباط الجوازات، وضباط الاستخبارات، وضباط الدفاع المدني، ومديري السجون والضباط فيها، وضباط حرس الحدود، وضباط قوات الأمن الخاصة، وضباط الحرس الوطني، وضباط القوات المسلحة، كل بحسب المهام الموكولة إليه في الجرائم التي تقع ضمن اختصاص كل منهم.

4 - محافظي المحافظات ورؤساء المراكز.

5 - رؤساء المراكب السعودية البحرية والجوية في الجرائم التي تُرتكب على متنها.

6 - رؤساء مراكز هيئة الأمر بالمعروف والنهي عن المنكر في حدود اختصاصهم.

7 - الموظفين والأشخاص الذين خولوا صلاحيات الضبط الجنائي بموجب أنظمة خاصة.

8 - الجهات واللجان والأشخاص الذين يُكلفون بالتحقيق بحسب ما تقضي به الأنظمة.

الفرع الثالث

إجراءات التحقيق المترتبة على حالة التلبس

يترتب على التلبس بعض إجراءات التحقيق منها القبض والتفتيش والقيام ببعض الإجراءات على سبيل الاستثناء.

أولاً: القبض في حاله التلبس:

نصت المادة 33 من الإجراءات الجزائية على أن: «لرجل الضبط الجنائي في حال التلبس بالجريمة، القبض على المتهم الحاضر الذي توجد دلائل كافية على اتهامه، على أن يُحرر محضراً بذلك، وأن يُبادر بإبلاغ هيئة التحقيق والادعاء العام فوراً. وفي جميع الأحوال لا يجوز إبقاء المقبوض عليه موقوفاً لأكثر من أربع وعشرين ساعة، إلا بأمر كتابي من المحقق».

فإذا لم يكن المتهم حاضراً، فيجوز لرجل الضبط الجنائي أن يصدر

أمراً بضبطه وإحضاره، وأن يُبيِّن ذلك في المحضر «ففي حالة التلبس بأي جريمة يجوز لرجل الضبط الجنائي القبض على المتهم وتفتيشه، ولو لم يصدر بشأنه مذكرة قبض من المحقق، لكن يجب المبادرة بإبلاغ هيئة التحقيق والادعاء العام فوراً».

كما أنه يجب على رجل الضبط الجنائي بعد قبضه على المتهم الحاضر الذي وجدت دلائل كافية على اتهامه أن يُحرر محضراً بذلك، وأن يسمع فوراً أقوال المتهم المقبوض عليه، والسؤال هنا هو الاستفسار عما إذا كان هو الذي ارتكب الجريمة، وأسباب ارتكابه لها، دون توجيه الأسئلة التفصيلية، أو مواجهته بالأدلة القائمة ضده، أو مواجهته بالشهود أو المتهمين الآخرين، فذلك داخل في الاستجواب، وهو محظور على رجل الضبط الجنائي مطلقاً، وإذا لم يأت المتهم المقبوض عليه بما يقنع رجل الضبط الجنائي أنه بريء؛ فإنه يجب على رجل الضبط أن يرسله خلال أربع وعشرين ساعة مع المحضر إلى المحقق[1].

أما إذا أتى المتهم المقبوض عليه في حالة التلبس بالجريمة بما يقنع رجل الضبط الجنائي أنه بريء؛ فلرجل الضبط الجنائي سلطة الإفراج عنه إن رأى ذلك، وبهذا يكون النظام قد أعطى رجال الضبط الجنائي سلطةً تقديرية واسعة في تقدير الإفراج من عدمه.

وهذا في المتهم الحاضر؛ أما إذا لم يكن المتهم أو الشريك المتلبس بالجريمة حاضراً في محل الجريمة أو قريباً منه؛ فيجب على رجل الضبط الجنائي أن يصدر أمراً بضبطه وإحضاره [2]، وأن يبيِّن ذلك في المحضر، ويتم تنفيذ هذا الأمر بواسطة رجال السلطة العامة، أو أحد المحضرين، ويُفترض تنفيذ القبض تخويل مَن يُباشر سلطة اتخاذ وسائل الإكراه بالقدر اللازم لتقييد حرية المقبوض عليه حتى لا يهرب، ولا يجوز استخدام الإكراه إذا كان

---

(1) مادة 34 اجراءات جزائية.

(2) مادة 33 اجراءات جزائية.

المقبوض عليه قد امتثل طواعية دون مقاومة.

ثانياً: إجراء التفتيش في حالة التلبس:

والتفتيش هو إجراء من إجراءات التحقيق لا الاستدلال، يهدف إلى التوصل إلى أدلة جريمة ارتكبت فعلاً، وذلك بالبحث عن هذه الأدلة في مستودع السر، سواء أجريَ على شخص المتهم أو في منزله دون التوقف على إرادته، والأصل أن تختص به هيئة التحقيق والادعاء العام ولا يجوز إجراءه إلا بعد الحصول على مذكره بالتفتيش منها، إلا أن النظام استثناءً جازه لرجل الضبط الجنائي في حالة التلبس بالجريمة، فأجاز له القبض على المتهم الحاضر الذي توجد دلائل كافية على اتهامه حيث نصت المادة 42 من نظام الإجراءات الجزائية على أن: «يجوز لرجل الضبط الجنائي – في الأحوال التي يجوز فيها القبض نظاماً على المتهم – أن يفتشه، ويشمل التفتيش جسده وملابسه وأمتعته. وإذا كان المتهم أنثى، وجب أن يكون التفتيش من قبل أنثى يندبها رجل الضبط الجنائي»، ويجوز أيضاً تفتيش منزل المتهم حيث نصت المادة 43 جزائية على أن: «يجوز لرجل الضبط الجنائي في حال التلبس بجريمة أن يفتش منزل المتهم ويضبط ما فيه من الأشياء التي تفيد في كشف الحقيقة، إذا أتضح من أمارات قوية أنها موجودة فيه، وإذا قام أثناء تفتيش منزل المتهم قرائن قويه ضده أو ضد أي شخص موجود فيه على أنه يخفي معه شيء يفيد كشف الجريمة جاز لرجل الضبط الجنائي أن يفتشه[1] أما إذا كان المتهم أنثى وجب أن يكون التفتيش من قبل أنثى يندبهارجل الضبط الجنائي، بخلاف ما تحمله من منقولات فيتم تفتيشه من قبل رجل الضبط الجنائي.

---

(1) مادة 44 جزائية.

المبحث الثالث

مرحلة المحاكمة في نظام الإجراءات الجزائية السعودي

المطلب الأوّل

مبدأ الفصل بين سلطة الاتهام والتحقيق

مفهوم المبدأ[1]:

الفصل بين سلطتي التحقيق والاتهام تعني: عدم جواز الجمع بين صفتي المحقق والمدّعي في الدعوى الجنائية في آن واحد، أي أن تتولى وظيفة التحقيق هيئة مستقلة عن وظيفة الادعاء، تلافياً لما يؤدي إليه التباين بين العمليتين حيث يوجد هذا التباين إذا قام بالإجراءين جهة واحدة هي (هيئة التحقيق والادعاء العام) في المملكة.

تطبق المبدأ في النظام:

بعد صدور قانون الإجراءات الجزائية الحالي، وإنشاء هيئة التحقيق والادعاء العام، أصبحت الأخيرة تتولى كأصل عام سلطتي التحقيق والاتهام في كافة الجرائم، واستثناءً من هذا الأصل العام في الاختصاص بمباشرة التحقيق الجنائي تخول بعض الأنظمة في المملكة جهات أخرى اختصاص خاص لإجراء التحقيق في بعض الجرائم التي تتعلّق بمهامها الوظيفية، كما أن هناك جرائم يعود سبب الاختصاص الخاص لجهات تتولى التحقيق فيها لاعتبارات أخرى منها الصفة الخاصة لمرتكبها كما هو الحال في جرائم العسكريين والأطباء.

---

(1) ضمانات المتهم فى مرحلة التحقيق الابتدائي فى النظام السعودي بحث للحصول على درجه الماجستير فى الأنظمة للباحث طه محمد عبد الله ابراهيم بجامعة الملك عبد العزيز بجدة عام 1427 هـ ص 90 وما بعدها.

المطلب الثاني

مبدأ علانية التحقيق بالنسبة للخصوم

المقصود بالمبدأ:

يُقصد بالمبدأ أن جميع إجراءات التحقيق تكون علانية بالنسبة للخصوم أو وكلائهم لضمان تحقيق نوع من الرقابة على التحقيق بالنسبة للخصوم وبث روح الطمأنينة لديهم وأيضاً إحاطتهم بجميع أدلة التحقيق ليتوافر لديهم الفرصة في الرد على هذه الأدلة وتجهيز دفاعهم.

الخصوم الذين يسري عليهم المبدأ:

نصت المادة 69 من نظام الإجراءات الجزائية على أن: «للمتهم والمجني عليه والمدَّعي بالحق الخاص ووكيل كل منهم أو محاميه، أن يحضروا جميع إجراءات التحقيق. وللمحقق أن يجري التحقيق بغيبة المذكورين أو بعضهم متى رأى ضرورة ذلك لإظهار الحقيقة، وبمجرد انتهاء الضرورة يُتيح لهم الاطلاع على التحقيق»، فبمقتضى هذه المادة فإن الخصوم الذي يحق لهم حضور التحقيق وجميع إجراءاته هم خصوم الدعوى سواء كان المتهم، أو وكيله، أو محاميه، أو كان المدَّعي بالحق الخاص، أو المجني عليه، أو وكلائهم أو محاميهم.

الاستثناء من المبدأ:

يُستثنى من مبدأ علانية التحقيق بالنسبة للخصوم، وأنه لا يجوز إجراء تحقيق إلا بحضورهم استثناء يتمثَّل في حاله الضرورة وحالة الاستعجال على النحو التالي.

أولاً: حاله الضرورة:

نصت المادة 69 إجراءات جزائية على أن: «.... وللمحقق أن يجري

التحقيق بغيبة المذكورين أو بعضهم متى رأى ضرورة ذلك لإظهار الحقيقة، وبمجرد انتهاء الضرورة يُتيح لهم الاطلاع على التحقيق، ويُقصد بحاله الضرورة طبقاً لمفهوم نص هذا المادة الحالة التي تستدعي اتخاذ إجراء للتحقيق بصفه ضرورية في غيبه الخصوم أو وكلائهم للكشف عن الحقيقة ويهدُف من هذا الإجراء عدم عرقلة سير التحقيق في الأسباب والظروف التي قد تؤدي إلى ذلك، فقرَّر المنظِّم جواز القيام ببعض إجراءات التحقيق في غياب الخصوم، وحيث أن المقرر أن حضور الخصوم التحقيق يُعد ضماناً من ضمانات التحقيق بالنسبة للمتهم والخصوم، وحتى لا يكون التحقيق الذي تم في غيبه الخصوم منافيا للعدالة قرر المنظِّم للخصوم ووكلائهم الاطلاع على التحقيق الذي تم في غيبتهم حتى يتثنى لهم اتخاذ اللازم حياله وتمكينهم من الرد عليه أو تجهيز دفاعهم بشأنه، ولم يُحدد النظام إجراءات معينة تتخذ في غيبة الخصوم، وإنما ترك ذلك لتقدير المحقق في كل ما يراه مناسباً لإظهار الحقيقة.

تقدير حاله الضرورة:

نصت اللائحة التنفيذية لنص المادة 69 جزائية على أن: «يعود تقدير حاله الضرورة للمحقق فبمقتضى ذلك ليس هناك شرائط محددة لتقدير حاله الضرورة بل تترك لكل ما يراه المحقق ضرورياً لإظهار الحقيقة».

ثانياً: حالة الاستعجال[1]:

وهذه في الحالة التي تدعو فيها ظروف التحقيق إلى ضرورة مباشرة إجراء من إجراءات التحقيق في غياب الخصوم على وجه الاستعجال التي لا يتمكن المحقق من إخطار الخصوم وتدعوا الحالة الملحة إجراء التحقيق مثال ذلك شهادة شاهد أوشك على الموت أو معاينة آثار الجريمة قبل أن تطمس آثارها أو قبل أن يتمكّن المتهم من إزالة آثارها.

---

(1) ظفير، سعد بن محمد، الإجراءات الجنائية في المملكه السعودية، الرياض طبعة 1424هـ.

المبحث الرابع

إجراءات التحقيق

يُقصد بالتحقيق المرحلة التي تتناول مجموعة الإجراءات التي تُباشرها سلطات التحقيق والتي تستهدف إلى جمع الأدلة للتثبت من وقوع الفعل الإجرامي ونسبته إلى شخص معين أو عدم حصولها أصلاً وتكيفها النظامي وتحديد مدى كفاية الأدلة لإقامة الدعوى الجزائية أو حفظها [1].

ويستلزم التحقيق في الجريمة إلى استجواب المتهم ومواجهته بالجريمة المسندة إليه وأيضاً سماع شهادة مَن شاهدو واقعه الجريمة، وقد يستلزم جمع الأدلة إلى تفتيش المتهم وتفتيش مسكنه، وقد يحتاج إلى مراقبة المحادثات الشخصية وتسجيلها أو ضبط المراسلات، وقد تحتاج الدعوى الجزائية أيضاً إلى الاستعانة بالخبراء المختصين، مثال ذلك المواد المخدرة يجب إحالة المادة المخدرة المضبوطة إلى الخبراء وسوف نُوضّح ذلك تفصيلياً في المطالب الآتية:

المطلب الأول

الاستجواب والمواجهة

الفرع الأول

مفهوم الاستجواب

عرف مشروع اللائحة التنفيذية لنظام الإجراءات الجزائية الاستجواب بأنه: «سؤال المتهم ومواجهته بالأدلة أو بغيره من المشاركين في الجريمة أو بالشهود، وذلك لإثبات التهمة أو نفيها»، فوفقاً لذلك أن الاستجواب هو

(1) عبد الخالق، حسن، أصول الإجراءات الجنائية، المرجع السابق.

إجراء من إجراءات التحقيق بمقتضاه يتم مناقشة المتهم تفصيلياً في التهم الموجهة إليه ومناقشته في الأدلة الموجهة ضده للرد عليها ومواجهته بالشهود وغيره من المشاركين معه في الجريمة، ويجب أن يشمل الاستجواب بصفته إجراء من إجراءات التحقيق العناصر الآتية[1]:

1 - التثبت من شخصية المتهم وإثبات البيانات الخاصة به من حيث الاسم ومحل الإقامة ومهنته ومواصفاته وكل البيانات الشخصية الخاصة بالمتهم، ويجب أن تُحيط هيئة التحقيق المتهم بالتهمة المسندة إليه [2] وذلك عن استجوابه لأول مرة في التحقيق.

2 - مواجهة المتهم بالأدلة المثبتة للاتهام ومناقشته تفصيلياً فيها.

3 - إثبات أقوال المتهم فيما اسند إليه وأيضاً إثبات دفاعه وطلباته التي تؤيد براءته.

الفرع الثاني

ضمانات الاستجواب في النظام السعودي

للأهمية التي تترتب عليها عملية الاستجواب فقد أحاط المنظِّم السعودي عمليه الاستجواب بمجموعة من الضمانات التي تكفل حياد الاستجواب وعد التأثيرَ فيه على إرادة المتهم، ونُوضحها على النحو التالي.

أولاً: إسناد الاستجواب إلى هيئه التحقيق فقط:

قصر المنظِّم السعودي إجراء الاستجواب إلى هيئة الادعاء العام

(1) ظفير، سعد بن محمد، الإجراءات الجنائية في المملكة السعودية، المرجع السابق.

(2) مادة 101 إجراءات جزائية.

والتحقيق دون غيرها حيث نصت المادة 14 جزائية على أن: «تتولى هيئة التحقيق والادعاء العام التحقيق والادعاء العام طبقاً لنظامها»، ونصت المادة 64 جزائية على أن: «يجب على المحقق أن يقوم بالتحقيق في جميع القضايا الكبيرة»، ونصت المادة 3 من نظام هيئة التحقيق على أن: «تختصه الهيئة وفقاً للأنظمة وما تحدد اللائحة التنظيمية على ما يلي: أ - التحقيق في الجرائم»، ولا يجوز لغيرها من رجال الضبط الجنائي إجراءه إلا في أحوال محدودة جداً.

ثانياً: جواز الاستعانة بوكيل أو محام في مرحلة الاستجواب:

نصت المادة 64 جزائية على أن: «للمتهم حق الاستعانة بوكيل أو محام لحضور التحقيق»، ونصت أيضاً المادة 4 جزائية على أن: «يحق لكل متهم أن يستعين بوكيل أو محام لحضور التحقيقات أو المحاكمة»، لضمان إجراء الاستجواب أجاز النظام للمتهم الاستعانة بوكيل أو محام لحضور التحقيقات حتى يكون المتهم على اطمئنان لسير عملية الاستجواب وعدم وجود أي إكراه مادي أو معنوي عليه، ويحق للمتهم ووكيله أو محاميه حضور كافة إجراءات التحقيق إلا ما يتعلّق بحالة الضرورة بإجراء التحقيق في غيبة الخصوم، وفي هذه الحالة يجب على المحقق تمكين المتهم أو محاميه من الاطلاع على التحقيق وكافة الإجراءات التي تمّت في غيبتهم[1]، ويجب على سلطات التحقيق أن تقدم كافة التسهيلات التي قد يحتاجها المحامي في الاطلاع على أوراق التحقيق، وكل ما يقتضيه المحامي للقيام بواجبه للدفاع عن المتهم، ولا يجوز بأي حال من الأحوال رفض طلبات المحامي المشروعة المتعلّقة بالتحقيق دون سبب مشروع للرفض[2]، ويجوز للمتهم للمحامي أن ينفرد بالمتهم، ولا يجوز بأي حال من الأحوال عزل المتهم عن محاميه في الاستجواب حيث نصت المادة 70 جزائية على أن: «ليس للمحقق أن يعزل المتهم عن وكيله أو

---

(1) ماده 69 إجراءات جزائية.

(2) مادة 19 من نظام المحاماة.

محاميه الحاضر معه في أثناء التحقيق. وليس للوكيل أو المحامي التدخل في التحقيق، إلا بإذن من المحقق. وله في جميع الأحوال أن يُقدِّم للمُحقِّق مُذكرة خطية بملاحظاتِه، وعلى المحقق ضم هذه المُذكِرة إلى ملف القضية» وتكون المهمة الأساسية للمتهم في الاستجواب هي مراقبة التحقيق لضمان حياديته ويحق للمحامى أن يبدي ملاحظاته على التحقيق في مذكرهة تضم لملف التحقيق كما وضحت المادة سالفة الذكر.

ثالثاً: سرعة استجواب المتهم:

من الضمانات أيضاً الخاصة بالمتهم سرعة استجوابه ومعرفة صدق التهمة من عدمها حتى لا يمكث رهن التحقيق بدون ذنب فعلي، فنصت المادة 34 جزائية على أن: «على رجل الضبط الجنائي أن يسمع فوراً أقوال المتهم المقبوض عليه فإن أتى بما يُبرئه أطلق سراحه وإلا أرسله إلى المحقق لاستجوابه خلال أربع وعشرين ساعة، ثم يأمر بإيقافه أو إطلاقه»؛ لأن الأصل براءة المتهم. لزم من ذلك سرعة استجوابه.

رابعاً: ضمان عدم التأثير على المتهم:

نصت المادة 102 جزائية: «يجب أن يتم الاستجواب في حال لا تأثير فيها على إرادة المتهم في إبداء أقواله، ولا يجوز تحليفه ولا استعمال وسائل الإكراه ضده. ولا يجوز استجواب المتهم خارج مقر جهة التحقيق، إلا لضرورة يُقدِرُها المحقق».

ونصت أيضاً اللائحة التنفيذية للمادة 2/102 على أن: «يراعي المحقق في تعامله مع المتهم احترام كرامته وآدميته، ولا يجوز استعمال وسائل الإكراه ضده، ولا استعمال عقاقير أو أجهزة أو عنف للحصول منه على ما يُدينه، وكل دليل يتم الحصول عليه بناءً على إكراه، أو وعد، أو وعيد، أو تهديد، أو أي وسيلة تشل الإرادة، أو تفقد الوعي لا يُعتد به، ولا بما يُسفر عنه في الإثبات».

المطلب الثاني

سماع الشهادة في التحقيق

الفرع الأوّل

مفهوم الشهادة وسلطه المحقق فيها

الشهادة في التحقيق الجنائي هي إدلاء أي شخص أمام هيئة التحقيق بكل ما اتصل بعلمه عن طريق حواسه من معلومات قد تُفيد في كشف الحقيقة في جريمة معينه وقد عرف مشروع اللائحة التنفيذية الشهادة في التحقيق الجنائي في بابها الأول بأنها إخبار مَن يُعتد بقوله لإثبات حق، أو نفيه.

أنواع الشهادة:

يوجد للشهادة ثلاث أنواع [1].

1 - الشهادة المباشرة:

وهي الشهادة التي ينقل فيها الشاهد مشاهدته المباشرة عن الحادث الجنائي وما أدركته حواسه عند وقوع الحادث وما اتصل به، وتعتبر الشهادة المباشرة هي الأصل في الشهادة؛ لأن الشاهد يروي ما أدركته حواسه عن الحادث الجنائي التي تصادفت وجوده في مكان وقوعه، وهذه الشهادة هي القاعدة في الإثبات، وهي التي يقوم عليها الدليل والحكم بناء عليه ولها الحجة في الإقناع والقوة التدليلية هي القناعة.

---

(1) النجار، عماد عبدالحميد، الادعاء العام والمحاكمة الجنائية وتطبيقاتها فى المملكة العربية السعودية، الرياض، طبعة 1417.

2 - الشهادة السمعية:

وهي الشهادة عن شاهد وهو أن شخص يرى حادث جنائي ويروي به إلى شخص آخر، فالشاهد في هذه الحالة لا يروي ما اتصل بعلمه الشخصي وما شاهده، بل يروي ما سمعه عن الشاهد الأصلي ورواه له، وهي تُسمى شهادة سمعية مثال على ذلك أن يروي المجني عليه في المستشفى إلى الطبيب أن الذي تعدّى عليه شخص معين ثم يموت، ففي هذه الحالة تعتبر شهادة الطبيب شهادة سمعية وقيمتها التدليلة مرتبطة باطمئنان القاضي لها، فيصح للقاضي أن يعتمد عليها في حكمة خاصة إذا كانت هناك أدلة تُعززها.

3 - شهادة السامع:

وهي الشهادة التي لا مصدر لها غير السامع وما يُردده الناس دون معرفة مصدرة فهي عبارة عن تنقل الاتهامات والكلمات دون معرفة أساس ذلك، فلا تنتقل عن شخص مباشر شاهد حدث الجريمة بنفسه وقيمة هذه الشهادة إنها ليست لها قوة تدليلية في الإثبات، ولكن ما هي إلا فتح طريق لرجال البحث الجنائي للبحث والتنقيب عن الحقيقة.

سلطة المحقق في سماع الشهود:

نصت المادة 95 جزائية على أن «على المحقق أن يستمع إلى أقوال الشهود الذين يطلب الخصوم سماع أقوالهم ما لم يرَ عدم الفائدة من سماعها. وله أن يستمع إلى أقوال مَن يرى لزوم سماعه من الشهود عن الوقائع التي تؤدي إلى إثبات الجريمة وظروفها وإسنادها إلى المتهم أو براءته منها»، بمقتضى ذلك يجوز لإطراف الدعوى الجزائية سواء كان المتهم أو المدَّعي بالحق الخاص أن يطلب من المحقق سماع شهود معينين قد يفيدوا في إظهار الحقيقة سواء بإثبات الجريمة أو نفيها [1]، إلا أن المنظِّم أعطى للمحقق السلطة الكاملة في مدى الاستجابة لطلبات الخصوم فيما يتعلق بسماع الشهود لضمان الجدية

(1) ظفير، سعد بن محمد، الإجراءات الجنائية في المملكه السعودية، المرجع السابق.

في التحقيق وعدم تضييع الوقت في سماع شهادة لا تفيد في التحقيق حيث نصت المادة 1/95 من مشروع اللائحة التنفيذية على أن: «إذا طلب أحد الخصوم سماع أقوال الشهود فيسأله المحقق عن الواقعة التي يُراد الشهادة فيها ؛ فإن قدَّر جدوى ذلك دعا الشاهد إلى الحضور، وإن لم يرَ فائدة من سماع الشهادة فله أن يرفض الطلب، وفي جميع الأحوال يتعين على المحقق أن يُثبت ذلك في محضر التحقيق»، ويجوز للمحقق من تلقاء نفسه استدعاء مَن يرى أن في شهادتهم إفادة في كشف الحقيقة دون طلب من الخصوم.

الفرع الثاني

إجراءات الشهادة في التحقيق الجنائي

إذا رأى المحقق أن هناك فائدة من إحضار الشهود في كشف الحقيقة فيتم استدعائهم واتباع الإجراءات المنصوص عليها نظامياً في الشهادة في التحقيق الجنائي، ويمكن حصرها في الآتي:

أولاً: إجراءات استدعاء الشهود وحضورهم:

1 - يتم تبليغ الشهود بقلم المحضرين، للحضور للشهادة أمامه بوساطة المحضرين، أو رجال السلطة العامة، أو أي وسيلة أخرى يراها المحقق.

2 - يجب أن يتم تبليغ الشهود قبل أربع وعشرين ساعة على الأقل من موعد سماع شهادتهم؛ ما لم يستدعِ الأمر الاستعجال، ويكون الإحضار وفق الإجراءات المنصوص عليها في نظام المرافعات[1].

---

(1) المادة 2/95 من مشروع اللائحة التنفيذية.

3 - يجب على كل مَن يُستدعى للشهادة الحضور أمام المحقق في المكان والزمان المحددان في طلب الحضور، وفي حالة امتناع الشاهد عن الحضور بدون عذر مقبول جاز لهيئة التحقيق أن تأمر بإحضاره باستثناء الشهادة في حد من حدود الله فلا يجبر الشاهد على الحضور[1].

4 - إذا كان الشاهد مريض أو لديه ما يمنعه من الحضور تُسمع شهادته في مكان وجوده، ويُرجى في تقدير العذر المانع للحضور إلى المحقق، ويجوز للمحقق أن ينتقل له أو يندب احد رجال الضبط الجنائي في الانتقال له وسماع شهادته في حالة الندب المنصوص عليها نظامياً في المادة 65، 66 جزائية، وإذا كان الشاهد المراد سماعه خارج النطاق المكاني للمحقق جاز للمحقق بعد الحصول على إذن رئيس فرع الهيئة التابع لها بندب المحقق التي تدخل الدعوى الجزائية في اختصاصه المكاني[2].

ثانياً: إجراءات سماع الشهادة أمام المحقق:

1 - يجب على المحقق أن يثبت البيانات الكاملة لكل شاهد ويجب أن تشمل تلك البيانات اسم الشاهد، ولقبه، وسنه، ومهنته، وجنسيته، ومحل إقامته، وصلته بالمتهم، أو المجني عليه، أو المدَّعى بالحق الخاص، وذلك طبقاً لما هو وارد في المادة 96 جزائية.

2 - يجب تدوين تلك البيانات والشهادة في (محضر تحقيق) من دون تعديل، أو محو، أو كشط، أو تحشير، وأن حدث ذلك يجب أن يصدق عليه المحقق والكاتب والشاهد[3].

---

(1) المادة 3/95 من مشروع اللائحة التنفيذية.

(2) نص المادة 100 جزائيه ومشروع اللائحة التنفيذية لها.

(3) مادة 96 جزائية ومشروع اللائحة التنفيذية لها.

3 - يُكتب في محضر التحقيق (محضر سماع شاهد)، ويُثبت تحته اسم المحقق، ووظيفته، واسم الكاتب، والمترجم إن وجد، وكل مَن حضر من أطراف القضية، ومكان تحرير المحضر، ويومه وتاريخه، وساعته.

4 - يطلب المحققُ من الشاهد الإدلاء بمعلوماته التي لها صلة بموضوع التحقيق، تركه يسترسل في إجابته وسرد ما لديه متعلّقاً بموضوع التحقيق، ولا يُقاطعه؛ ما لم يخرج عن موضوع السؤال، وذلك دون التأثير على إرادته بأية وسيلة.

5 - إذا فرغ الشاهد من شهادته ناقشه المحقق فيها بالقدر الذي يتحقق به صحة هذه الشهادة، ولا يظهر أمام الشاهد بمظهر المتشكك في أقواله، ويستوضح قدر الإمكان من الشاهد عن زمان ومكان الحادث، والفاعل، وكيفية وقوعه، والباعث له.

6 - تتم كتابة أقوال الشاهد وأجوبته عن الأسئلة المطروحة عليه في محضر التحقيق، وتُتلى عليه ليصادق عليها.

7 - يضع كل من المحقق والكاتب إمضاءه على الشهادة، وكذلك الشاهد بعد تلاوتها عليه، فإن امتنع عن وضع إمضائه أو بصمته أو لم يستطع يثبت ذلك في المحضر مع ذكر الأسباب التي يبديها [1].

8 - يستمع المحقق لكل شاهد على انفراد، وله أن يُواجه الشهود بعضهم ببعض وبالخصوم [2].

9 - على المحقق في حال حضور الشهود منع اتصالهم ببعض، وإذا فرغ من الاستماع إلى شاهد فيبقيه على انفراد؛ حتى ينتهي من

(1) مادة97 جزائية.

(2) مادة98 جزائية ومشروع اللائحة التنفيذية لها

سماع بقية الشهود الحاضرين.

10 - يجوز للمحقق أن يُواجه الشهود بعضهم ببعض، وبالخصوم، أو أن تكون المواجهة شخصية؛ بأن يذكر لكل شخص ما قاله الآخر، وكلاهما ماثل أمام المحقق، وإذا أصر كل منهما على موقفه فعلى المحقق إثبات ذلك في المحضر، وإن عدل أحدهما عن أقواله وجبت مناقشته عن هذا العدول، ويُثبت المحقق جميع ما يصدر من الأشخاص الذين تجري بينهم المواجهة من تصرفات أو أقوال.

11 - للخصوم بعد الانتهاء من الاستماع إلى أقوال الشاهد إبداء ملحوظاتهم عليها، ولهم أن يطلبوا من المحقق الاستماع إلى أقوال الشاهد عن نقاط أخرى يُبينونها. وللمحقق أن يرفض توجيه أي سؤال لا يتعلق بالدعوى، أو يكون في صيغته مساس بأحد [1].

12 - في حاله الرغبة في توجيه أسئلة إلى الشاهد من الخصوم توجَّه الأسئلة من المحقق، وتُثبَت مع إجابتها في محضر التحقيق، ويجوز أن يكون توجيهها مباشرة من الخصم؛ ما دامت تحت إذن المحقق.

حالات الإعفاء من الشاهدة في النظام:

1 - لا يجوز للمهنيين كالمحامين والأطباء الشهادة بالمعلومات التي اتصلت بهم بسبب وأثناء تأدية مهنتهم حيث نصت المادة.

2 - لا يجوز إجبار أحد في الشهادة في حد من حدود الله.

---

(1) مادة 99 جزائية ومشروع اللائحة التنفيذية لها.

المطلب الثالث

أمر التوقيف

الفرع الأول

مفهوم التوقيف ومبرراته

لم يرد التوقيف: لإجراءات الجزائية السعودي كغيره من الأنظمة تعريف للتوقيف ويمكن القول أن التوقيف هو إيداع المتهم في السجن فترة التحقيق كلها، أو بعضها إلى أن تنتهي محاكمته[1] بمقتضى ذلك التوقيف هو سلب حرية المتهم فترة من الزمن غالباً ما تتصف بالتأقيت تستوجبه مصلحة التحقيق وِفق ضوابط قرَّرها المنظِّم[2] ولا يُعتبر التوقيف في ذاته عقوبة؛ لأنه قد يتخذ قبل أن تثبت إدانة المتهم، بل يُعتبر وسيلة إكراه تستعمل لمصلحة الدعوى الجزائية، والضرورة هي المبرر الوحيد للتوقيف[3]، مع ملاحظة أن التوقيف لا يُعتبر عقوبة على الرغم من اتحادهما في طبيعة العقوبة، وهي سلب الحرية ولكنه إجراء يهدُف للمحافظة على المتهم والتحفُّظ عليه لمصلحة التحقيق ويدخل ضمن سلطات التحقيق.

مبررات التوقيف:

التوقيف يكون على أشخاص لم تثبت إدانتهم بعد، وقد تظهر براءتهم

---

(1) سرور، احمد فتحي، الوسيط في الإجرءات الجنائية، دار النهضة العربية، القاهرة 1985م.

(2) الشهاوي، قدري عبدالفتاح ضوابط الحبس الاحتياطي، منشئة المعارف، بالاسكندرية، 2003.

(3) ظفير، سعد بن محمد، الإجراءات الجنائية في المملكه السعودية، المرجع السابق.

والمبرر من توقيفهم قد يكون حماية التحقيق لعدم التأثير عليه أو تقييد حرية المتهم إذا خيف عليه الهرب، أو حماية المتهم نفسه، أو إرضاء للشعور العام حيث نصت المادة 113 جزائية على أن: «إذا تبين بعد استجواب المتهم، أو في حالة هروبه، أن الأدلة كافية ضده في جريمة كبيرة، أو كانت مصلحة التحقيق تستوجب توقيفه لمنعه من الهرب أو من التأثير على سير التحقيق..»؛ ولهذا فإن هناك عدة مبررات للتوقيف وهي:

1 - التوقيف وسيلة لضمان عدم هروب المتهم وتنفيذ العقوبة:

يُعتبر التوقيف وسيلة لضمان تنفيذ العقوبة للحيلولة دون هروب المتهم من العقاب، وخاصة إذا كان المتهم مجهول الهوية أو غير معلوم له محل إقامة، وأيضاً يُمثِّل التوقيف ضمان لاستكمال إجراءات التحقيق إذا خيف هرب المتهم وذلك لإظهار الحقيقة

2 - حماية المتهم:

يُمثِّل التوقيف في بعض الأحيان حماية للمتهم؛ لأنه قد تتعرَّض حياته للخطر من قِبل المجني عليه، أو عائلته، أو من أفراد المجتمع، وذلك إذا كان الفعل المنسوب للمتهم تُثير حافظة المجني عليه، أو عائلته مما قد يدفعهم للانتقام.

3 - المحافظة على الأدلة:

التوقيف يمنع المتهم من العبث بالأدلة وسير إجراءات التحقيق، فقد يمنعه من إخفاء، أو تلفيق الأدلة، أو اتصاله بالشهود، والتأثير عليهم هذا بالإضافة أن بقاء المتهم تحت تصرُّف المحقق يساعد على إنجاز التحقيق بسرعة[1]، كما قد يكون التوقيف حائل بين المتهم للاتصال بشركائه في الجريمة للاتفاق معهم على إخفاء أدلة الجريمة.

---

(1) الزهني، لأدور غالي، الاجرءات الجنائية، الطبعة الثالثة، مكتبة غريب بالقاهرة، 1990م.

4 - تهدئة الرأي العام:

يعمل التوقيف على تهدئة الرأي العام في الجرائم التي تُثير حافظة الرأي العام وتُشعرهم بالاطمئنان على أن المتهم سينال عقابه، وخاصة إذا كان المتهم ذا خطورة إجرامية حتى يشعرهم بأن المتهم لن يستطيع الإقدام على مثل هذه الحالة مرة أخرى حيث نص قرار صاحب السمو الملكي وزير الداخلية في لائحة أصول الاستيقاف والحجز المؤقت والتوقيف الاحتياطي بالقرار رقم 233 في 1404/1/17 هـ في المادة 11/د على أن: «إذا كان بقاؤه طليقاً يُشكل خطراً على حياته، أو حياة غيره، أو يؤدي إلى الإساءة للأمن العام، أو يُحدث هياجاً أو بلبلة بين الناس».

الفرع الثاني

الجرائم الموجبة للتوقيف

أولاً: الجرائم الموجبة للتوقيف هي الجرائم الكبيرة التي يجب فيها على المحقق إيقاف المتهم، وهي لا تخضع للسلطة التقديرية للمحقق، ومن حيث تحديد تلك الجرائم نصت المادة 112 من نظام الإجراءات الجزائية على أن: «يُحدد وزير الداخلية بناء على توصية رئيس هيئة التحقيق والادعاء العام ما يُعد من الجرائم الكبيرة الموجبة للتوقيف» وقد صدر قرار صاحب السمو الملكي وزير الداخلية الذي حدَّد في الجرائم الكبيرة الموجبة للتحقيق بناء على توصية رئيس هيئة التحقيق والادعاء العام طبقاً لنص المادة 112جزائية وهي [1]:

(1) قرار وزير الداخلية رقم 1900 وتاريخ 1428/7/9هـ بناء على توصية رئيس هيئة التحقيق والإدعاء العام بموجب المادة 112 جزائية.

أولاً: الجرائم الكبيرة الموجبة للتوقيف هي:

1 - الحدود المعاقب على العمد. قتل أو بالقطع.

2 - القتل العمد أو شبه العمد.

3 - جرائم الإرهاب والجرائم المخلة بأمن الدولة.

4 - قضايا المخدرات والمؤثرات العقلية، أو الأسلحة والذخائر، أو تزييف وتقليد النقود، أو التزوير، أو الرشوة أو انتحال صفة رجل السلطة العامة، أو غسل الأموال. المعاقَب على أي منها نظاماً بسجن يزيد عن سنتين.

5 - سرقة السيارات.

6 - القوادة أو إعداد أماكن للدعارة.

7 - ترويج المسكرات، أو قصد الترويج في حال تهريبها، أو تصنيعها، أو حيازتها.

8 - اختلاس الأموال الحكومية، أو أموال الشركات المساهمة أو البنوك أو المصارف ما لم يرد المبلغ المختلَس.

9 - الاعتداء عمداً على ما دون النفس الناتج عنها زوال عضو، أو تعطيل منفعة أو جزء منها، أو إصابة مدة الشفاء منها تزيد عن خمسة عشر يوماً، ما لم يتنازل صاحب الحق الخاص.

10 - الاعتداء عمداً على الأموال أو الممتلكات الوظيفته، الخاصة بأي وسيلة من وسائل الإتلاف بما يزيد قيمة التالف عن خمسة آلاف ريال، ما لم يتنازل صاحب الحق الخاص.

11 - الاعتداء على رجل الأمن أثناء مباشرته مهام وظيفته، أو الإضرار بمركبته الرسمية، أو بما يستخدمه من تجهيزات.

12 - استعمال أو إشهار السلاح الناري بقصد الاعتداء به على الأنفس.

13 - انتهاك حرمة المنازل بالدخول بقصد الاعتداء على النفس، أو العرض، أو المال.

14 - انتهاك الأعراض بالتصوير والنشر، أو التهديد بالنشر.

15 - الاعتداء على أحد الوالدين بالضرب ما لم يحصل التنازل.

الفرع الثالث

الجرائم الجائز فيها التوقيف

هي الجرائم التي يخضع فيها التوقيف إلى سلطة المحقّق التقديرية، وهي ليست لها حصر، ويجوز فيها التوقيف حتى وإن كانت من الجرائم الصغيرة، وتخرج هذه الجرائم عن الجرائم السابق تحديدها الموجبة للتوقيف التي تخرج عن السلطة التقديرية للمحقّق - الجرائم الكبير الموجبة للتوقيف - ويمكن تحديد الأسباب التي يجوز على أثرها للمحقّق إيقاف المتهم في الآتي:

1 - إذا لم يكن للمتهم محل إقامة معلوم يجوز للمحقّق إيقاف المتهم احتياطياً حتى إن كان ذلك في الجرائم الصغيرة الغير موجبة للتوقيف؛ حيث نصت المادة 108 من نظام الإجراءات الجزائية على أن: «إذا لم يكن للمتهم محل إقامة معروف فعليه أن يُعين محلاً يقبله المحقّق، وإلا جاز للمحقّق أن يُصدر أمراً بإيقافه».

2 - إذا خيف هرب المتهم أو تأثيره على سير التحقيق يجوز للمحقّق إيقافه لمصلحة التحقيق حيث نصت المادة 113 جزائية على أن

«إذا تبيّن بعد استجواب المتهم، أو في حالة هروبه، أن الأدلة كافية ضده في جريمة كبيرة، أو كانت مصلحة التحقيق تستوجب توقيفه لمنعه من الهرب، أو من التأثير في سير التحقيق؛ فعلى المحقّق إصدار أمر بتوقيفه مدةً لا تزيد على خمسة أيام من تاريخ القبض عليه»، مع ملاحظة أن مصلحة التحقيق التي وردت في نص المادة تنطبق على الجرائم الكبير والصغيرة؛ لأن المنظّم أورد مصلحة التحقيق كسبب مستقل دون النظر من أن الأدلة تكفي لاتهام المتهم في جريمة كبيرة أم لا؛ لأن الجرائم الكبيرة موجبة للتوقيف بقوة النظام ولا تخضع لسلطة المحقّق بغض النظر عن مصلحة التحقيق، ونلاحظ أن المنظّم في المادة 2/113 من مشروع اللائحة التنفيذية خالف ذلك؛ حيث قصر سبب مصلحة التحقيق الذي يخضع للسلطة التقديرية للمحقّق واجب على المحقّق مراعاته فقط في الجرائم الكبيرة حيث نصت المادة على أن: «توقيف المتهم لمنعه من الهرب، أو التأثير في سير التحقيق لا يكون إلا في الجرائم الكبيرة»، رغم أن الجرائم الكبير موجبة للتوقيف كما ذكرنا ولا تخضع للسلطة التقديرية للمحقق.

الفرع الرابع

سلطة إصدار أمر التوقيف

تختلف سلطة إصدار أمر التوقيف باختلاف المرحلة التي تمر بها الدعوى الجزائية، فإذا كانت الدعوى الجزائية في مرحلة التحقيق ولم تتصل بالمحكمة بعد، فتختص هيئة التحقيق وحدها دون غيرها بإصدار، أما إذا أُحيلت واتصلت الدعوى بالمحكمة انتقل الحق بالتوقيف أو الإفراج إلى المحكمة ونبيّن ذلك على النحو الآتي:

1 - المحقِّق:

سلطة إصدار أمر التوقيف هو حق المحقِّق وحده أثناء التحقيق ولا يجوز لغيره من رجال الضبط الجنائي أو غيرهم مما يجوز ندبهم في التحقيق إصداره؛ لأن إصدار أمر التوقيف يستلزم استجواب المتهم والاستجواب حق أصيل للمحقِّق حتى في الأحول التي يجوز فيها الندب لا يحق للمندوب استجواب المتهم، وبالتالي لا يحق له توقيفه حيث نصت المادة 6/65 من مشروع اللائحة التنفيذية على أن: «ليس للمحقِّق أن يندب رجل الضبط الجنائي لإجراء المواجهة، أو الأمر بالتوقيف الاحتياطي».

2 - المحكمة:

إذا خرجت الدعوى الجزائية من سلطة المحقِّق واتصلت بالمحكمة في هذه الحالة يكون صاحب الحق في توقيف المتهم أو الإفراج عنه إذا كان موقوفاً للمحكمة حتى وإن كانت المحكمة التي أُحيلت إليها الدعوى الجزائية غير مختصة نوعياً أو مكانياً؛ لأن سلطة هيئة التحقيق بالنسبة لتوقيف المتهم يكون انتهى بقرار الإحالة منهي إلى المحكمة ولا يبقى لها إلا سلطة مباشرة الدعوى الجزائية أمامها حيث نصت المادة 123 جزائية على أن: «إذا أُحيل المتهم إلى المحكمة يكون الإفراج عنه إذا كان موقوفاً أو توقيفه إذا كان مفرَجاً عنه من اختصاص المحكمة المحال إليها، وإذا حكم بعدم الاختصاص تكون المحكمة التي أصدرت الحكم بعدم الاختصاص هي المختصة بالنظر في طلب الإفراج، أو التوقيف، إلى أن ترفع الدعوى إلى المحكمة المختصة».

● ويجدر الإشارة إلى أنه إذا لم ينتهِ التحقيق في مدة التوقيف المحدَّدة نظاميا لهيئة التحقيق، وهي ستة شهور يجب على الهيئة إحالة الدعوى إلى المحكمة والمحكمة تقرر اللازم من حيث تكملة إجراءات التحقيق، وأيضاً إيقاف المتهم أو الإفراج عنه حيث نصت المادة 1/114 من مشروع اللائحة التنفيذية التي نصت على: «إذا انتهت مدة توقيف المتهم المنصوص عليها في هذا النظام في وقت الكشف الطبي على المتهم من أجل علاجه، أو بيان

حالته العقلية؛ فيُحال إلى المحكمة المختصة؛ لاتخاذ ما تراه من الأمر بتوقيفه لاستكمال التحقيق».

الفرع الخامس

مدة أمر التوقيف

قيَّد المنظِّم السعودي مدة أمر التوقيف الصادرة من المحقِّق بحد أقصى لمدة خمسة أيام حيث نصت المادة 113 جزائية على أن: «إذا تبيَّن بعد استجواب المتهم فعلى المحقِّق إصدار أمر بتوقيفه مدةً لا تزيد على خمسة أيام»، ويجوز تجديدها لمدة أو لمدد أخرى إذا رأى المحقِّق مصلحة للتحقيق في ذلك بحيث لا تزيد عن أربعين يوماً بناء على أمر مُسبب من رئيس فرع هيئة التحقيق والادعاء العام في الدائرة التي يتبعها المحقِّق حيث نصت المادة 114 جزائية على أن: «ينتهي التوقيف بمضي خمسة أيام، إلا إذا رأى المحقِّق تمديد مدة التوقيف، فيجب قبل انقضائها أن يقوم بعرض الأوراق على رئيس فرع هيئة التحقيق والادعاء العام بالمنطقة ليصدر أمراً بتمديد مدة التوقيف مدة أو مدداً مُتعاقبة، على الّا تزيد في مجموعها على أربعين يوماً من تاريخ القبض عليه»، وإذا تبيَّن الحاجة إلى إبقاء المتهم موقوفاً يجوز تجديد مدة إيقافه لمدد أطول لا تزيد المدة عن ثلاثين يوماً ولا تزيد في مجموعها عن ستة أشهر بناء على أمر رئيس هيئة التحقيق والادعاء العام الذي يرفع إليه الأمر، ونصت على ذلك المادة 114 التي نصت على: «..... وفي الحالات التي تتطلَّب التوقيف مدة أطول يرفع الأمر إلى رئيس هيئة التحقيق والادعاء العام ليصدر أمره بالتمديد مدة أو مدداً متعاقبة لا تزيد أي منها على ثلاثين يوماً، ولا يزيد مجموعها على ستة أشهر من تاريخ القبض على المتهم»، وبناء على ذلك يمكن تحديد مدة التوقيف بناء على مصدر الأمر على النحو الآتي:

1 - **رجل الضبط الجنائي:** في الأحوال التي يجوز له نظامياً

القبض فيها على المتهم لا يجوز إبقاء المتهم أكثر من 24 ساعة حيث نصت المادة 33 جزائية على أن: «.. لرجل الضبط الجنائي في حال التلبُّس بالجريمة القبض على المتهم الحاضر الذي توجد دلائل كافية على اتهامه؛ على أن يُحرِّر محضراً بذلك، وأن يُبادر بإبلاغ هيئة التحقيق والادعاء العام فوراً وفي جميع الأحوال لا يجوز إبقاء المقبوض عليه موقوفاً لأكثر من أربع وعشرين ساعة إلا بأمر كتابي من المحقِّق... »، ويبدأ سريان هذه المدة من وقت القبض.

2 - **المحقِّق**: مدة التوقيف الجائزة له خمسة أيام دون الرجوع إلى أحد، مع ملاحظة إذا كانت الجريمة لا تستوجب التوقيف مطلقاً يحق للمحقِّق أن يوقفه 24 ساعة، وهي المدة اللازمة لاستجواب المتهم ومدة 24 ساعة المقررة للمحقِّق تختلف عن المدة المقررة لرجل الضبط الجنائي، وتبدأ من تاريخ العرض على المحقِّق وذلك طبقاً لنص المادة 34 ومشروع اللائحة التنفيذية لها.

3 - **رئيس فرع التحقيق**: الذي يتبعه المحقِّق مدة خمسة أيام تُجدَّد لمدد أخرى بحيث لا تزيد عن أربعين يوماً من تاريخ القبض، فالسلطة الفعلية التي خولها له النظام هي 35 يوماً إذا أُضيف عليها الخمسة أيام المقررة بسلطة المحقِّق أصبح أربعين يوماً الواردة في نص المادة؛ لأن مدة الأربعين يوماً تُحسب من تاريخ القبض، وليس من تاريخ انتهاء المدة المقررة للمحقِّق.

4 - **رئيس هيئة التحقيق والادعاء العام**: مدة لا تزيد عن ثلاثين يوماً يجوز أن تُجدَّد لمدد أخرى بحيث لا تزيد عن ستة شهور من تاريخ القبض، والسلطة الفعلية المخولة لرئيس الهيئة هي أربعة أشهر وعشرة أيام إذا أُضيف عليها 40 يوماً المخولة للمحقِّق ورئيس الفرع أصبحت 6 شهور الواردة في نص المادة؛ لأنه كما

ذكرنا تُحسب 6 شهور من تاريخ القبض.

5 - **المحكمة:** عند اتصال الدعوى الجزائية بالمحكمة يكون صدور أمر التوقيف والإفراج للمحكمة المحال إليها الدعوى والمدة المقررة للمحكمة هي 21 يوماً، ويجوز تجديدها إلى مدة أو مدد متلاحقة حيث نصت المادة 10/123 من مشروع اللائحة التنفيذية على أن: «مدة التوقيف القصوى في أمر الإيقاف الصادر من المحكمة هي واحد وعشرون يوماً، ويجوز تجديدها مدداً مماثلة بأوامر أخرى، وهكذا، ويكون نهائياً».

الفرع السادس

شروط صدور أمر التوقيف

هناك عدة شروط يجب مراعتها وتوافرها قبل صدور أمر التوقيف من المحقّق وإلا كان أمر التوقيف باطل، وهذه الشروط قد تكون شكلية، أو موضعية على النحو التالي:

أ - الشروط الشكلية:

تتمثّل الشروط الشكلية في الآتي:

1 - بيانات الأمر الصادر بالتوقيف:

يجب أن يشمل أمر التوقيف اسم الشخص المراد توقيفه وبياناته كاملة وأيضاً اسم المحقّق الذي أصدره والخاتم الرسمي، وتكييف الجريمة المسندة إلى المتهم والأدلة التي ضده، وبيان تاريخ القبض، وتحديد مدة الإيقاف، وأيضاً يجب أن يشمل أمر التوقيف على أمر بتكليف مأمور دار التوقيف بقبول المتهم عنده وذلك طبقاً لنص المادة 3/113 من مشروع اللائحة التنفيذية التي

نصت على: «يصدر أمر التوقيف من المحقِّق، ويجب أن يشتمل على ما يأتي:

(1) اسم الشخص المطلوب توقيفه رباعياً، وجنسيته، ومهنته، ومحل إقامته، وبصمته، وتاريخ الأمر.

(2) اسم المحقِّق، وتوقيعه، والختم الرسمي.

(3) تكييف الجريمة المسندة إلى المتهم.

(4) تسبيب أمر التوقيف.

(5) بيان تاريخ القبض على المتهم.

(6) تحديد مدة التوقيف.

(7) تكليف مأمور التوقيف بقبول المتهم في دار التوقيف، ووضعه فيها .

مع ملاحظة أن هناك حالات لا يستطيع المحقِّق الحصول فيها على الاسم الصحيح للمتهم في حالة ضبط المتهم متلبساً بارتكاب جريمة معينة وكانت الأدلة المتوفرة كافية لتوقيفه ولا يمكن الاستدلال على هويته لرفضه الإدلاء بها وعدم الاهتداء لمعرفة اسمه، فيمكن إصدار أمر بتوقيفه على أنه مجهول الهوية طالما كانت شخصيته محددة بما لا يدع مجالاً للخطأ فيها وذلك حتى تثبت شخصيته الحقيقة فيما بعد[1].

2 - ضرورة تسبيب أمر التوقيف [2]:

لأن الأمر بالتوقيف الاحتياطي أمراً استثنائياً، فيجب أن يكون له ما يُبرره؛ لذلك فإنه يجب على مصدره أن يبيِّن أسباب إصداره لهذا الأمر خاصة وأنه يُمثِّل اعتداءً على حق أصيل للفرد، وهو افتراض أصل البراءة في

(1) الشهاوي، قدري عبدالفتاح ضوابط الحبس الاحتياطي، المرجع السابق.

(2) العكيلي، عبد الأمير، أصول الإجراءات الجنائية في قانون أصول المحاكمات الجزائية، ج1، ط1، مطبعة المعارف، بغداد، 1975م.

المتهم حتى تثبت إدانته بحكم قضائي بات.

ولم يرد نص صريح في نظام الإجراءات الجزائية السعودي يوجب تسبيب أمر التوقيف من المحقّق إلا أن نص المادة 36 جزائية أوجبت على إدارة السجون أو دار التوقيف بعدم قبول أي أمر بالتوقيف ما لم يكن مسبباً ويُفهم من ذلك أنه من الضرورة على المحقّق تسبيب أمر التوقيف حيث نصت على أن: «... ولا يجوز لإدارة أي سجن أو دار توقيف قبول أي إنسان إلا بموجب أمر مُسبب ومحدَّد المدة موقَّع عليه من السلطة المختصة».

3 - ضرورة إبلاغ المتهم بأسباب توقيفه:

بموجب نص المادة 116 من نظام الإجراءات الجزائية التي يستوجب إبلاغ الموقوف فوراً بأسباب القبض عليه أو توقيفه حيث نصت على أن: «يُبلغ فوراً كل مَن يُقبض عليه أو يوقف بأسباب القبض عليه أو توقيفه، ويكون له حق الاتصال بمَن يراه لإبلاغه، ويكون ذلك تحت رقابة رجل الضبط الجنائي».

وجاء في مشروع اللائحة التنفيذية للنظام من خلال المادة 1/116 ويجب على المحقّق إيراد أسباب القبض على المتهم، أو توقيفه في محضر التحقيق ويوقّع المتهم في المحضر على العلم بها.

4 - تحديد التوقيف بمدة معينة:

من الشروط الشكلية الهامة في أمر التوقيف يجب أن يكون أمر التوقيف مؤقت محدَّد بمدة معينة حيث نصت المادة 36 على أن: «ولا يجوز لإدارة أي سجن أو دار توقيف قبول أي إنسان إلا بموجب أمر مُسبب ومحدَّد المدة موقع عليه من السلطة المختصة»، ومن حيث تحديد المدة الواردة في أمر التوقيف ما نصت عليه المادة 114 كما ذكرنا سابقاً في مدة أمر التوقيف.

ب - الشروط الموضوعية للتوقيف:

1 - أن تكون هناك جريمة وقعت بالفعل:

يجب أن يكون هناك جريمة وقعت بالفعل وأن تكون هناك دلائل كافية موجة للمتهم، ووجود دلائل كافية على الاتهام شرط في نظام الإجراءات الجزائية السعودي للأمر بالتوقيف، وهو ما تطلبته المادة113 من نظام الإجراءات الجزائية السعودي التي تنص على أنه: «إذا تبيَّن بعد استجواب المتهم، أو في حالة هروبه، أن الأدلة كافية ضده في جريمة كبيرة..... » ويقصد بالدلائل الكافية الأمور التي يدل ثبوتها على توافر العناصر التي تكفي لإصدار أمر التوقيف أو قيام شبهات مستندة إلى ظروف واقعية تؤدي للاعتقاد بصدور الجريمة من المتهم[1].

2 - ضرورة استجواب المتهم[2]:

يجب أن يسبق صدور أمر التوقيف استجواب المتهم؛ لأن استجواب المتهم عمل من أعمال التحقيق ويقصد به مواجهة المتهم بأدلة الاتهام الموجَّهة ضده ومناقشته فيها مناقشة تفصيلية فينكرها إذا كان منكرا للتهمة أو يعترف بالتهمة إذا شاء الاعتراف، وعلى ذلك فإنه بالاستجواب تظهر الحقيقة فإذا اقتنع بدفاع المتهم أخلى سبيله وإلا أمر بوقفه احتياطياً إذا اقتضت مصلحة التحقيق ذلك، والاستجواب وجوبي قبل حبس المتهم وفقاً لنص للمادة 113من نظام الإجراءات الجزائية السعودي والتي نصت على أنه: «إذا تبيَّن بعد استجواب المتهم، أو في حالة هروبه أن الأدلة كافية ضده في جريمة كبيرة، أو كانت مصلحة التحقيق تستوجب توقيفه لمنعه من الهرب أو من التأثير في سير التحقيق، فعلى المحقِّق إصدار أمر بتوقيفه مدة لا تزيد على خمسة أيام من تاريخ القبض عليه».

(1) الشهاوي، قدري عبدالفتاح ضوابط الحبس الاحتياطي، المرجع السابق.

(2) الشريف، عمر واصف، النظرية العامة في التوقيف الاحتياطي، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2004م.

● ويُستثنى من وجوب استجواب المتهم قبل توقيفه إذا كان المتهم هارباً وقبض عليه في هذه الحالة يجوز للمحقِّق إصدار أمر بتوقيفه دون استجواب وذلك طبقاً لنص المادة 113 كما ذكرنا حيث نصت على: «إذا تبيَّن بعد استجواب المتهم، أو في حالة هروبه.... ».

3 - وجود أسباب كافية للتوقيف:

بالإضافة إلى ما سبق يجب أن تكون هناك أسباب كافية تستدعي توقيف المتهم وهذه الأسباب هي أن تكون مصلحة التحقيق تقتضي ذلك أو إذا خيف هرب المتهم أو التأثير على سير التحقيق، وسبق أن وضحنا ذلك في الجرائم الواجب والجائز فيها التوقيف.

الفرع السابع

مكان التوقيف والرقابة على تنفيذه

التوقيف يكون في دار التوقيف المعدَّة لهذا الغرض حيث نصت المادة الأولى من نظام السجن والتوقيف على أن: «.... ويودع مَن يصدر بشأنه أمر توقيف من السلطات المختصة دور التوقيف، وذلك وفقاً لأحكام هذا النظام ولائحته التنفيذية»، ونصت أيضاً المادة 118 جزائية على أن: «لا يجوز لمأمور السجن أو دار التوقيف أن يسمح لأحد رجال السلطة العامة بالاتصال بالموقوف إلا بإذن كتابي من المحقِّق، ولا يجوز تنفيذ أمر التوقيف خارج السجن أو في مكان التوقيف المخصص»، لذلك حيث نصت المادة 39 جزائية على أن: «لكل مَن علم بوجود مسجون، أو موقوف بصفة غير مشروعة أو في مكان غير مخصص للسجن أو التوقيف أن يبلغ هيئة التحقيق والادعاء العام» ،ويُفهم من هذا النص أنه لا يجوز تنفيذ التوقيف خارج المكان المخصص له وأن هيئة التحقيق هي المختصة بالرقابة على تنفيذ أمر التوقيف، لأن الرقابة

على السجون وعلى دور التوقيف من اختصاص هيئه التحقيق والادعاء العام حيث نصت المادة 37 جزائية على أن: «على المختصين من أعضاء هيئة التحقيق والادعاء العام زيارة السجون ودور التوقيف في دوائر اختصاصهم في أي وقت دون التقيُّد بالدوام الرسمي، والتأكُّد من عدم وجود مسجون أو موقوف بصفة غير مشروعة، وأن يطلعوا على سجلات السجون ودور التوقيف، وأن يتصلوا بالمسجونين والموقوفين، وأن يسمعوا شكاواهم، وأن يتسلموا ما يُقدمونه في هذا الشأن. وعلى مأموري السجون ودور التوقيف أن يقدموا لأعضاء هيئة التحقيق والادعاء العام كل ما يحتاجونه لأداء مهامهم».

الفرع الثامن

إجراءات وضمانات التوقيف

تُعتبر شروط أمر التوقيف الشكلية والموضوعية المذكورة بعاليه من إجراءات وضمانات المتهم في التوقيف، وكذلك أيضاً حصر سلطة أمر التوقيف في جهة معينة مُتمثّلة في هيئة التحقيق أو المحكمة، وأيضاً تحديد مدة أمر التوقيف وأسبابه والجرائم التي يجوز فيها التوقيف، يُعد من الضمانات الهامة للمتهم بالإضافة إلى ذلك يوجد بعض الإجراءات والواجبة الاتباع وتُعدّ من ضمانات المتهم أيضاً في أمر التوقيف على النحو الآتي:

1 - يجب عند صدور أمر بتوقيف المتهم أن يسلم أصل أمر التوقيف لمأمور دار التوقيف بعد توقيعه على صورة هذا الأمر بالتسلُّم وتودع الصورة في ملف القضية، لا يجوز لمأمور السجن أو دار التوقيف أن يسمح لأحد رجال السلطة العامة بالاتصال بالموقوف إلا بإذن كتابي من المحقِّق، وعليه أن يدون في دفتر السجن اسم الشخص الذي سُمِح له بذلك ووقت المقابلة وتاريخ الإذن

ومضمونه[1] ولا يجوز للمحقِّق قبول أي موقوف لديه بغير إذن، ويحقُّ لكل فرد علم.

2 - في الأحوال التي يصدر فيها قرار من المحقِّق بعدم اتصال المتهم بأحد وعدم جواز السماح لأحد بزيارته إذا اقتضت مصلحة التحقيق ذلك لا يجوز الإخلال بحق المحامي أو وكيل المتهم بزيارته ويكون اتصال المتهم بوكيله أو محاميه بموجب إذن مكتوب من المحقِّق، بناءً على طلب المتهم، أو طلب وكيله، أو محاميه، وفي كل الأحوال لا يجوز أن يسري الأمر بمنع اتصال المتهم بأحد أكثر من 60 يوم[2].

3 - يجوز للموقوف احتياطياً التظلُّم من أمر توقيفه، أو أمر تمديد التوقيف؛ إذا كان صادراً من غير لجنة إدارة الهيئة؛ ويقدم بطلب إلى رئيس دائرة التحقيق التابع لها المحقِّق، أو رئيس الفرع، أو رئيس الهيئة حسب الأحوال[3].

4 - ضرورة حسم مدة التوقيف من العقوبة: ومن الضمانات الهامة المترتِّبة على التوقيف الاحتياطي للمتهم ضرورة حسم مدة التوقيف التي يقضيها من مدة عقوبته؛ لأن التوقيف الاحتياطي يسلب حرية المتهم وذلك من أجل مصلحة التحقيق، فإن خصم مدة التوقيف الاحتياطي من مدة العقوبة إجراء لتحقيق العدالة وإلا كان الحبس الاحتياطي عقوبة تُضاف إلى العقوبة المحكوم بها على المتهم، ويفهم ذلك من نص المادة 216 من قانون الإجراءات الجزائية السعودي والتي نصت على: «يُفرج في الحال عن المتهم الموقوف إذا كان الحكم صادر بعدم الإدانة، أو بعقوبة لا يقتضي

(1) مادة 15، 18 من نظام الاجرءات الجزائية.
(2) راجع نص المادة 119 جزائية ومشروع لائحتها التنفيذية.
(3) مادة 3/116 من مشروع اللائحة التنفيذية.

تنفيذها السجن، أو إذا كان المتهم قد قضى مدة العقوبة المحكوم بها في أثناء توقيفه»[1].

5 - ومن الضمانات الهامة للموقوف احتياطياً أجاز نظام الإجراءات الجزائية للموقوف تقديم شكوى لأي سبب يراه في دار التوقيف مثل سوء المعاملة أو غيرها من الأسباب حيث نصت المادة 38 جزائية على أن: «لكل مسجون أو موقوف الحق في أن يقدم في أي وقت لمأمور السجن، أو دار التوقيف شكوى كتابية أو شفهية، ويطلب منه تبليغها إلى عضو هيئة التحقيق والادعاء العام، وعلى المأمور قبولها وتبليغها في الحال بعد إثباتها في سجل مُعد لذلك، وتزويد مقدمها بما يُثبت تسلُّمها، وعلى إدارة السجن أو التوقيف تخصيص مكتب مستقل لعضو الهيئة المختص لمتابعة أحوال المسجونين أو الموقوفين».

6 - يجب أن يتم تنفيذ أمر التوقيف خلال ثلاثة أشهر من إصداره حيث نصت المادة 117 جزائية على أن: «لا يجوز تنفيذ أوامر القبض، أو الإحضار، أو التوقيف، بعد مضي ثلاثة أشهر من تاريخ صدورها ما لم تُجدد».

الفرع التاسع

حق الموقوف في التظلم من قرارات سلطة التحقيق

نظّم مشروع اللائحة التنفيذية لنظام الإجراءات الجزائية السعودي

(1) العكيلي، عبد الأمير، أصول الإجراءات الجنائية في قانون أصول المحاكمات الجزائية، المرجع السابق.

هذا الحق حيث جعل من حق الموقوف التظلم من أمر توقيفه، حيث نصت المادة (3/116) على أنه: «للموقوف احتياطياً التظلم من أمر توقيفه إلى لجنة الهيئة..... ويقدم بطلب إلى رئيس دائرة التحقيق التابع لها المحقق، أو رئيس الفرع أو رئيس الهيئة حسب الأحوال، ويُحال التظلم مع أوراق القضية للبت فيه من اللجنة المذكورة، وعليها البت في التظلم خلال خمسة أيام من تاريخ تقديمه»[1].

واللجنة المذكورة في الفقرة (م2/63) تُشكَّل من ثلاثة أعضاء في مرتبة أعلى من مرتبة المحقِّق مصدر الأمر، أو سابقين له في الأقدمية إذا كانوا في مرتبة واحدة».

وهذه الفقرة نظَّمت حق الموقوف احتياطيا بالتظلم من أمر توقيفه أو من أمر تحديد التوقيف وذلك شرط بأن يكون أمر التوقيف صادراً من غير لجنة إدارة الهيئة، فإذا كان صادراً من هذه اللجنة فلا يحقُّ له التظلم، وإذا كان أمر التوقيف صادراً من غير اللجنة المشار إليها والمشكلة من ثلاث أعضاء في مرتبة أعلى من مرتبة المحقِّق مصدر الأمر أو السابقين له في الأقدمية إذا كانوا في مرتبة واحدة، جاز للموقوف التظلم من أمر التوقيف أمام هذه اللجنة. ويُفهم مما سبق أن التظلم يُقدم باسم هذه اللجنة إلى رئيس دائرة التحقيق التابع لها المحقِّق، أو رئيس دائرة التحقيق التابع لها المحقِّق، وإذا باشر التحقيق رئيس دائرة التحقيق قدم التظلم إلى رئيس الفرع، وإذا باشر التحقيق رئيس الفرع قدم التظلم إلى رئيس الهيئة وفي كل الأمور يجب أن يُحال التظلم مع أوراق القضية إلى لجنة إدارة الهيئة فهي المختصة بالبت فيه وعليها أن تفصل في هذا التظلم خلال خمسة أيام من تاريخ تقديمه.

---

(1) الشريف، عمر واصف، النظرية العامة في التوقيف الاحتياطي، المرجع السابق.

المبحث الخامس

إحالة الدعوى الجزائية إلى المحكمة المختصة

المطلب الأول

مفهوم الإحالة

قرار الإحالة هو أمر يصدر من المحقِّق بمقتضاه يُحيل المتهم للمحاكمة أمام المحكمة المختصة بناء على الأدلة الواردة في محضر التحقيق.

فإذا توصَّل المحقِّق بعد انتهاء التحقيق أن الأدلة على الاتهام كافية لرفع الدعوى الجنائية أصدر أمر برفعها إلى الجهة القضائية المختصة، وإذا قام برفعها إلى المحكمة المختصة يُكلف المتهم بالحضور أمامها سواء كان المتهم موقوفاً أو مفرَّج عنه [1].

ويتولى المدعي العام مباشرة دعوى الحق العام أمام الجهة القضائية المختصة بموجب لائحة يبرز فيها الوقائع الثابتة في القضية والأوصاف الإجرامية، وأدلتها والنشاط الإجرامي للمتهم، مع الإشارة إلى النصوص الشرعية والنظامية للعقوبة المنطبقة وطلب إنزالها بحق المتهم [2].

وإذا اشتمل التحقيق على أكثر من جريمة واحدة من اختصاص محاكم متماثلة الاختصاص، وأتت مرتبطة كأن يكون المتهم قد ارتكب جريمتين كالسرقة غير الحدية والضرب، فهنا تُحال الأوراق جميعها بأمر إحالة واحد إلى المحكمة المختصة مكاناً بأحدها (المحكمة الجزئية). أما إذا اشتمل التحقيق

---

(1) المادة 126 جزائية.

(2) تاج الدين، مدني عبد الرحمن، أصول التحقيق الجنائي وتطبيقاتها في المملكة، ص286، الرياض، معهد الإدارة، 1425هـ.

على أكثر من جريمة واحدة من اختصاص محاكم مختلفة الاختصاص، كما لو كان المتهم قد ارتكب جريمة السرقة الحدية والضرب، فهنا تُحال الأوراق جميعها بأمر إحالة واحد إلى المحكمة الأوسع اختصاصاً وهي المحكمة العامة[1] حيث نصت المادة127 جزائية على أن: «إذا شمل التحقيق أكثر من جريمة من اختصاص محاكم متماثلة الاختصاص وكانت مرتبطة فتُحال جميعها بأمر إحالة واحد إلى المحكمة المختصة مكاناً بإحداها، فإذا كانت الجرائم من اختصاص محاكم مختلفة الاختصاص فتُحال إلى المحكمة الأوسع اختصاصاً».

المطلب الثاني

بيانات قرار الإحالة

إذا تبيَّن للمحقِّق كفاية الأدلة التي تُرجِّح فعل المتهم للجريمة فيصدر قراراً باتهامه يجب أن يتضمَّن اسم المحقِّق الذي أصدره، واسم المتهم، وشهرته، وعمره، ومحل ولادته، وإقامته، ومهنته، وجنسيته، ورقم وتاريخ ومصدر هويته، وتاريخ القبض عليه، وبداية مدة توقيفه، وتوضيح ما إذا كان موقوفاً بسبب آخر، وبيان الوقائع الجريمة المؤثرة في الدعوى، وإجراءات التحقيق التي نجم عنها دليل، وذلك بما يوضِّح دور المتهم وجميع المساهمين في الجريمة، ويخلص المحقِّق في قراره إلى توجيه الاتهام، مع بيان الأدلة والقرائن التي يستند عليها، وذكر كافة الظروف والأسباب المشدِّدة أو المخفِّفة التي تنطبق على الفاعل، أو أحد المساهمين معه، وكذلك المستند الشرعي أو النظامي الذي يُعاقب على ارتكابها، وطلب إثبات ذلك، والحكم على المتهم

(1) العكيلي، عبد الأمير، أصول الإجراءات الجنائية في قانون أصول المحاكمات الجزائية، المرجع السابق.

بالعقوبة التي يستحقها شرعاً أو نظاماً[1].

مع ملاحظة ما نصت عليه المادة 2/126 من اللائحة التنفيذية التي نصت على أن: « تُرفع القضية إلى لجنة إدارة الهيئة لمراجعته إذا تضمَّن قرار الاتهام طلب توقيع عقوبة إتلافية على المتهم، وللجنة إدارة الهيئة توجيه المحقِّق بما تراه مناسباً في القضية، ولها كافة الصلاحيات المسندة للمحقِّق في هذا النظام، وإذا لم يتضمَّن قرار الاتهام طلب توقيع عقوبة إتلافية فيُرفع إلى اللجنة المذكورة في الفقرة (م 2/63) من هذه اللائحة لمراجعته، ولها أن تتَّخذ أحد هذه الإجراءات:

1 – أن تؤيِّد قرار الاتهام، وتأمر بالإحالة.

2 – أن تأمر بإجراء تحقيق تكميلي في مسائل تُحدِّدها للمحقِّق.

3 – أن تُصدر قرارا الحفظ مسبباً ؛ وفق ما يقضي به هذا النظام ولائحته.

---

(1) مادة 1/126 من مشروع اللائحة التنفيذية.

المبحث السادس

المحكمة الرقمية ومشكلة الاختصاص

تخضع قواعد القانون الجنائي في تطبيقها من حيث المكان لمبدأ الإقليمية، ويعني خضوع الجرائم التي تقع في إقليم دولة معينة لقانونها الجنائي النافذ، بحيث تصبح محاكمها هي صاحبة الولاية بنظر الدعوى الناشئة عنها، ولا تخضع من حيث الأصل لسلطان أي قانون أجنبي، وفي المقابل لا يمتد سريان قانون الدولة الجنائي خارج نطاقها الإقليمي وفقاً لحدودها المعترَف بها في القانون الدولي إلّا في أحوال استثنائية اقتضتها حماية المصالح الجوهرية للدولة، أو متطلّبات التعاون الدولي في مكافحة الإجرام، والأصل أن عناصر الركن المادي للجريمة تكتمل في مكان واحد، أو بالأحرى في نطاق إقليم دولة واحدة، حيث يقع السلوك الإجرامي (النشاط)، وتترتّب عليه آثاره الضارة في إقليم دولة واحدة، كأن يقدم أحدهم على طعن المجني عليه أو إطلاق الرصاص عليه، ما يفضي إلى وفاته في الحال أو بعد لحظة وجيزة، ومن ثم تعتبر الجريمة مرتكبة في هذا المكان. وعلى ضوء ذلك يتحدَّد القانون الواجب التطبيق، وبالتبعية المحكمة المختصة بنظر الدعوى[1].

وبعض الجرائم تتجاوز حدود مبدأ الإقليمية، حينما يتجزأ ركنها المادي أو يتوزَّع على أكثر من مكان بحيث يمكن وقوع السلوك في مكان، وليكن إقليم دولة (س)، في حين تتحقَّق النتيجة الإجراميَّة الضارة في نطاق إقليم دولة (ص)، ومن أمثلة ذلك أن يُطلق شخص النار من داخل الأراضي الليبية تجاه آخر موجود على الأراضي المصرية، فيُرديه قتيلاً أو العكس، ويتجلّى

---

(1) تاج الدين، مدني عبد الرحمن، أصول التحقيق الجنائي وتطبيقاتها في المملكة، المرجع السابق.

ذلك في عدد من الجرائم العابرة للحدود الإقليمية للدول والقارات، مثل جرائم تلويث البيئة البحرية والهوائية، والاتجار بالمخدرات، وغسل الأموال والقرصنة المعلوماتية وما إليها، ولقد حاول الفقه منذ زمناً بعيد، لحل مشكلة تنازع القوانين، وانقسم الرأي إلى ثلاثة اتجاهات، فذهب الاتجاه الأول إلى أن العبرة في تحديد مكان وقوع الجريمة بالمكان الذي وقع فيه السلوك بقطع النظر عن المكان الذي تحقّقت فيه النتيجة، أو من المفترض تحقّقها فيه، وفي المقابل ذهب اتجاه آخر إلى أن مكان وقوع الجريمة يتحدّد بالمكان الذي تحقّقت فيه النتيجة أو كان من المفترض تحقّقها فيه، وبين هذا وذاك انبرى اتجاه ثالث إلى أن العبرة في ذلك تكون بمكان حصول أي منهما (السلوك أو النتيجة)، ولكل مذهب من هذه المذاهب مبرراته وأسانيده التي تُعزّزه وتدعمه[1].

(1) صالح، نائل عبد الرحمن، محاضرات في قانون أصول المحاكمات الجزائية، ط1، دار الفكر العربي، عمان، 1997م.

المبحث السابع

اتجاهات الفقه في اختصاص المحكمة الرقمية

إن مسألة الاختصاص في جرائم المعلوماتية عبر الوطنية، وما يمكن أن يُثيره من مشكلات تعدَّدت فيه آراء الفقه إلى المذاهب التالية:

المطلب الأول

مذهب السلوك الإجرامي

إن مذهب السلوك الإجرامي بوصفه معياراً لتحديد مكان وقوع الجريمة:

وفقاً لهذا المعيار، ينعقد الاختصاص للمحكمة التي يقع في نطاقها النشاط الإجرامي، وليس مكان حصول النتيجة أو الآثار المترتِّبة عليه؛ بدعوى أن اتخاذ آثار الفعل كمناط لتحديد مكان وقوع الجريمة تكتنفه بعض الصعوبات ؛ يمكن إجمالها في أنه معيار مرن وفضفاض، فضلاً عن أن معيار حصول النشاط أدعى إلى تيسير عملية الإثبات وجمع أدلة الجريمة، وأن المحكمة التي لها ولاية نظر الدعوى تكون قريبة من مسرح الجريمة. ناهيك أن الحكم الذي يصدر في الواقعة يكون أكثر فعالية ويسهل معه ملاحقة الجناة [1].

ويُضيف المؤيدون لهذا الاتجاه حججاً أخرى، منها أن حدوث الضرر

---

(1) عقيدة، محمود أبو العلا، شرح قانون الإجراءات الجنائية، الأردن، دار الحكمة، ط 2001م.

في مكان معين مردّه في الغالب أسباب لا إرادة لمقترف السلوك فيها، وأن من شأن تطبيق قانون الدولة التي تحقق في نطاقها الضرر لا يتفق واعتبارات العدالة نظراً لجهل الجاني بهذا القانون الذي يتم إعماله بحقه، وفي الغالب ليس ممكناً العلم به؛ إذ حينما أقدم على ارتكاب الفعل الذي أتاه يعتقد مشروعيته وفقاً لقانون البلد الذي وقع فيه السلوك، وإذا به غير ذلك من منظور قانون البلد الذي تحقّق فيه الضرر، وقد حظي هذا الاتجاه بتأييد جانب كبير من الفقه سواء في فرنسا أو مصر، ليس هذا فحسب، بل اتجهت بعض التشريعات المقارنة إلى تبنّيه، ومن هذا القبيل القانون الدولي الخاص النمساوي الصادر سنة 1979م والمجري الصادر في السنة ذاتها [1]

المطلب الثاني

مذهب النتيجة الإجرامية

يرى أنصار مذهب مكان تحقق النتيجة كمناط لتحديد الاختصاص أنه على الرغم من الحجج التي ساقها المذهب الأول، فإن هذا الاتجاه تعرض لجملة من الانتقادات من جانب آخر من الفقه، وقد انصبّت هذه الانتقادات على أن هذا المذهب لا يُعير اهتماماً للمكان الذي تحقق فيه الضرر أو أثر النشاط الإجرامي الذي كان الجاني يسعى إلى تحقيقه فيه. فالآثار الضارة هي التي تبعث الفزع في نفوس الناس، في حين أن مكان وقوع السلوك لا يعدو أن يكون مصدر الضرر ليس إلاّ، كما أن تمام الجريمة لا يكون إلا

(1) السعيد، كامل، شرح الأحكام العامة في قانون العقوبات الأردني والقانون المقارن، الطبعة الثانية، دار الفكر للنشر والتوزيع، عمان، 1983م.

في المكان الذي ظهرت فيه آثارها الضارة التي كان الجاني يقصدها أو يرغب في تحقيقها. يُضاف إلى ذلك أن تقادم الجريمة يتم احتسابه من الوقت الذي تحقّقت فيه النتيجة (الضرر)، كما يؤخذ في الحسبان جسامة الضرر كأساس لتقدير التعويض ولا عبرة بخطورة الفعل أو درجة الخطأ. كذلك يُعد حصول الضرر شرطاً أساسياً لقيام المسئولية المدنية، فتنفي هذه المسئولية متى ما انتفى الضرر، ومن ثَم لا مصلحة للمدعي في الدعوى، ما يجعلها بالتالي غير مقبولة [1].

ومن المبرِّرات التي سيقت لتعزيز هذا الاتجاه أن الأخذ به يُحقِّق وحدة الجريمة وعدم الفصل بين عناصرها، كذلك يمتاز هذا الاتجاه في نظر المدافعين عنه بأنه أكثر واقعية على اعتبار أن الضرر له مظهر خارجي ملموس خلافاً للنشاط الذي قد لا يكون كذلك متى ما اتخذ صورة الامتناع أو السلوك السلبي. ومن هنا، فقد لقي هذا الاتجاه ترحيباً من بعض الفقه إلى جانب ذلك تم تبنِّيه من بعض التشريعات المقارنة، ومنها القانون الألماني الصادر في 5 ديسمبر 1975م، والقانون الدولي الخاص التركي الصادر سنة 1982م. كما أقرّته اتفاقية بروكسل لسنة 1969 بشأن المسئولية عن أضرار التلوث بالبترول [2].

بالإضافة إلى ذلك دأب القضاء على تطبيقه في بعض المناسبات، من ذلك في واقعة عرضت على القضاء الأمريكي مؤداها أن قام رئيس فرقة باليه وهو على متن مركب أمريكي على قتل شخص موجود بمركب أجنبي بإطلاق النار عليه، وعند تقديمه للقضاء قضى بعدم اختصاصه بهذا الفعل مؤسساً ذلك على أن الوفاة (النتيجة) قد تحقّقت على متن مركب أجنبي، كما تكرر ذلك في واقعة أخرى مفادها أن شخصاً يحمل الجنسية الإنجليزية قُدِّم إلى المحاكمة أمام

(1) السعيد، كامل، شرح الأحكام العامة في قانون العقوبات الأردني والقانون المقارن، المرجع السابق.

(2) رمضان، مدحت، جرائم الاعتداء على الاشخاص والانترنت، دار النهضة العربية، القاهرة، 2000م.

إحدى محاكم ولاية ماسوشيست الأمريكية عن تهمة القتل العمدي التي قضت باختصاصها بنظر الدعوى عن الواقعة المذكورة، على الرغم من أن النشاط حصل على متن مركب إنجليزي في عرض البحر، في حين أن وفاة المجني عليه جراء هذا الفعل تمّت إثر وصوله إلى الولاية المذكورة [1].

المطلب الثالث

المذهب المختلط

أمام الانتقادات التي تعرض لها كلا المذهبين السابقين، برز اتجاه ثالث مفاده أن الجريمة تُعد واقعة في مكان حصول النشاط (العمل التنفيذي)، وكذلك المكان الذي تحقّقت فيه النتيجة أو الذي من المتوقع أو من المنتظر تحققها فيه. وهذا الاتجاه حظي بمباركة أغلب الفقه، ويجد مبرره في أن الركن المادي للجريمة يقوم على ثلاثة عناصر، وهي الفعل (النشاط)، والنتيجة، وعلاقة السببية، ما يعني أن الجريمة تُعد واقعة في كل مكان تحقق فيه عنصر من عناصر الركن المادي، أي في مكان النشاط ومكان النتيجة على حد سواء. وهذا الاتجاه أخذت به بعض التشريعات المقارنة، ومنها قانون العقوبات النرويجي وكذلك الدنمركي، والصيني والألماني والإيطالي لسنة 1930م. كما تبنّته المحاكم في بعض الدول ومنها فرنسا في عدد من الأحكام؛ إذ ذهبت إلى أن اختصاصها يتّسع ليشمل كل الأمكنة التي كانت مسرحاً للجريمة عند وقوعها. فقد قضي بأن المحكمة تعتبر مختصة بالدعوى الناشئة عن جريمة إصدار صك دون مقابل الوفاء فيما يخص صكاً

---

(1) السعيد، كامل، شرح الأحكام العامة في قانون العقوبات الأردني والقانون المقارن، المرجع السابق.

كان محرراً خارج فرنسا ومسحوباً على أحد البنوك فيها [1].

ولو عمد أحدهم إلى قتل آخر فأطلق النار من الأراضي المصرية تجاه المجني عليه الموجود على الأراضي الليبية ثم أُسعف المصاب إلى دولة ثالثة (ولتكن إيطاليا مثلاً) لتلقّي العلاج، وتوفي هناك، فإن الاختصاص ينعقد وفقاً للاتجاه السابق لكل من القانون المصري والليبي على حد سواء، على اعتبار أن المجني عليه كان موجوداً على إقليمها وقت مباشرة النشاط، ومن ثم فهذا المكان الذي اختاره لتنفيذ جريمته هو الذي ينبغي الاعتداد به، وبالتالي يتحدَّد القانون الواجب التطبيق على أساسه. وهنا، يتم تغليب قانون محل تحقق النتيجة إذا كانت الجريمة تامة، ومن قبيل ذلك جرائم السلوك والنتيجة (الجرائم المادية)، في حين يفضل مكان النشاط أو السلوك إذا كانت الجريمة قد وقفت عند حد الشروع أو كانت من قبيل جرائم السلوك المجرَّد.

---

(1) Sicber (U.): Les crimes informatiques et d' autres crimes dans le dommaine de la technologie informatique, Rev. int. dr. pen. 1993, p 53.

المبحث الثامن

المحكمة الرقمية والحلول المقترحة بشأن تنازع الاختصاص

إن الشبكة المعلومات العالمية (الانترنت) لا تستأثر بها دولة بعينها، ويتسنى لمستخدميها ولوجها من أية بقعة في العالم تقريباً من خلال جهاز حاسوب يكون متصلاً بها. فهي بطبيعتها باعتبارها موزّعة على أرجاء الكرة الأرضية لا تحدُّها حدود، ومن ثَم والأمر كذلك تكون من حيث المبدأ خارج أية رقابة أو سيطرة من أية جهة، وهذا يستتبع ولو نظرياً عدم إمكان خضوعها لسلطان قانون جنائي معين، وعملاً بمبدأ الإقليمية، فإن كل دولة تُمارس سيادتها على إقليمها بتطبيق قوانينها داخل حدودها، بصرف النظر عن جنسية مرتكب الجريمة، الذي يحتمل معه تنازع القوانين حيال الواقعة الواحدة، والذي يستتبع بالضرورة تنازع الاختصاص، وبالذات فيما يتّصل بالجرائم عبر الوطنية التي تُرتكب عبر شبكة الانترنت. فجريمة السبّ مثلاً عبر الرسائل الإليكترونية E. Mails تقع أحياناً في بلد ويتلقّاها الضحية في بلد آخر. وهنا ينبغي أن نُشير إلى أن هذه الرسائل والانترنت، دوات الاتصال عن بعد بواسطة هذه الشبكة تمر في كثير من الأحيان بأكثر من دولة قبل وصولها إلى بلد الاستقبال. ناهيك أن بعض الأفعال التي تُبث من خلال الانترنت، تُعد أحياناً جريمة في بلد ومباحة في غيره من البلدان المرتبطة بهذه الشبكة [1].

ومن الأمثلة التي يسوقها الفقه على ذلك أن الدعاية للقنّب الهندي (الخشخاش) أمر غير محظور في بعض البلدان كما هو الحال في هولندا، وفي المقابل يُعد مثل هذا السلوك مما يجرّمه القانون وغير مسموح به في

---

(1) البربري، صالح أحمد، دور الشرطة في مكافحة جرائم الإنترنت في إطار الاتفاقية الأوروبية، الموقعة في بودابست في 2001/11/23 – www. arablawinfo. com

بلدان أخرى بما فيها ليبيا وفرنسا مثلاً. والأمر ذاته ينسحب على المراهنات على كرة القدم، فهي غير مشروعة في بلد كفرنسا، وجائزة في بلدان أخرى كما هو الحال في إنجلترا ومما يزيد من حدّة المشكلة انعدام أو ضعف الرقابة على الرسائل الإليكترونية، وغياب قانون محدد يجري إعماله على مثل هذه الأفعال، ما من شأنه أن يبعث على التساؤل عن القانون الواجب التطبيق على المواقع الإليكترونية على شبكة الانترنت، وتطبيقاً للقواعد التي تحكم الاختصاص المكاني، فإن جرائم الانترنت العابرة للحدود Transnational Crimes تخضع في كثير من الأحيان لأكثر مَن قانون، فإذا وقع السلوك في نطاق بلد معين والآثار الضارة تحقّقت في نطاق بلد آخر، فإن كلا البلدين يكون قانونه واجب التطبيق على الواقعة، بمعنى أنه يتم تطبيق قانون كل دولة تحقّق في نطاقها أحد عناصر الركن المادي للجريمة (السلوك أو النتيجة)، فيكفي ليكون قانون البلد واجب التطبيق تلقّي الضحية الرسالة الإليكترونية المجسدة لجريمة السبّ أو التهديد مثلاً في نطاقه ولو كان الفعل ذاته غير معاقَب عليه في بلد المنشأ، وبتطبيق ذلك على جريمة نسخ المصنّفات ينعقد الاختصاص للدولة التي تم فعل النسخ على إقليمها، باعتبار أن النسخ عن بعد يُعد أحد العناصر المكونة لجريمة التقليد [1].

وثمة أمر فحسب، زيد الأمر تعقيداً وصعوبة في تحديد الاختصاص في جرائم الانترنت عبر الوطنية بالذات ألا وهو تباين المعايير الوطنية فيما يتعلّق بتحديد الاختصاص، الأمر الذي يفضي عادة إلى حدوث تنازع في الاختصاص بشأن هذه الطائفة من الجرائم، فعلى سبيل المثال، لو أن شخصاً ارتكب أياً من هذه الجرائم على إقليم دولة لا يحمل جنسيتها، فقد يحدث التنازع بين قانون الدولة التي ارتُكِبت الجريمة على إقليمها وقانون الدولة التي ينتمي إليها، أي أن الفعل يتنازع قانونان، قانون دولة الإقليم على أساس مبدأ الإقليمية، وفي الوقت ذاته قد يخضع لقانون دولة الجاني عملاً بمبدأ

(1) عبد المطلب، ممدوح عبد الحميد، جرائم استخدام شبكة المعلومات العالمية (الجريمة عبر الانترنت)، المرجع السابق.

الشخصية الإيجابية. ليس هذا فحسب، بل قد ينعقد الاختصاص لدولة ثالثة متى كانت الجريمة ماسّة بمصالحها الحيوية وفقاً لمبدأ العينية [1].

وقد طرح القضاء الأمريكي على شاكلة القضاء المقارن، وتصدّى لها في أكثر من مناسبة. ففي القضاء الأمريكي، تُشير التطبيقات القضائية إلى أنه يكفي لامتداد ولاية القضاء المذكور إلى جريمة وقعت في الخارج أن تكون آثارها قد مسّت مصالح أمريكية أو عرضتها للخطر، تأسيساً على مبدأ الاختصاص الشخصي. من ذلك ما قضت به المحكمة العليا لولاية نيويورك بصدد جريمة انتهاك قانون المستهلك والدعاية الخادعة. والمبدأ ذاته كان قد طُبِّق في واقعة أخرى مؤداها قيام إحدى الشركات بولاية بنسلفانيا بالادعاء على أحد مزوّدي الانترنت في ولاية كاليفورنيا بدعوى الاعتداء على علامة مسجلة في الولاية الأولى، وقد أسّست المحكمة حكمها على أن قضاء بنسلفانيا ينعقد له الاختصاص الشخصي على اعتبار أن مزود خدمة الانترنت له مشتركون في الولاية، بعبارة أخرى، فإن القانون الأمريكي يتّسع نطاق تطبيقه بحيث يمتد إلى الأفعال المرتكبة في الخارج طالما أن آثارها تحقّقت في الولايات المتحدة الأمريكية [2].

وتكرس هذا الاتجاه القضائي فيماانتهت إليه الدائرة الخامسة الاستئنافية في قضية قمار ومراهنات عبر الانترنت وقد اعتبر القضاء المذكور مجرد وضع برمجية فك التشفير (PGP) على الانترنت بمثابة تصدير لها، وهو ما يخول المحاكم الأمريكية التصدي لها باعتبارها صاحبة الاختصاص، بصرف النظر عن مكان وضع البرمجية [3].

(1) الشافعي، محمد إبراهيم محمد، النقود الإليكترونية، مجلة الأمن والحياة، أكاديمية الشرطة، دبي، س 12، ع1، يناير، 2004م.

(2) عبد المطلب، ممدوح عبد الحميد، جرائم استخدام شبكة المعلومات العالمية (الجريمة عبر الانترنت)، المرجع السابق.

(3) جريدة الرأي الأردنية، «قرصان إنترنت في قمة تشيلي»، جريدة الرأي، العدد 9568، 1996.

كما تبنّى القضاء الإنجليزي حلولاً مشابهة، فهو يختص بنظر الدعاوى الناشئة عن إساءة استخدام الانترنت، متى كان ثمة ارتباط بين الواقعة المرتكبة وبريطانيا عملاً بقانون إساءة استخدام الحاسب الصادر سنة 1990م (The Computer Misuse Act of 1990). الذي ينظم اختصاص المحاكم الإنجليزية، فيكفي امتداد آثار الواقعة إلى بريطانيا، ولو كانت هذه الواقعة قد حدثت في الخارج، وبصرف النظر عن محل إقامة الجاني. بعبارة أخرى، يكفي أن يكون ناتج عمله أو أن نيته منصرفة إلى أن يكون ناتج عمله تعديلاً محظوراً في حاسب موجود في بريطانيا (1). أما في فرنسا فيمتد اختصاص القضاء هناك إلى جرائم الانترنت التي وقعت في الخارج عملاً بقانون العقوبات الجديد متى كانت الظروف الواقعة تُبرر مصلحة فرنسا في إعمال قانونها عليها (2).

إن الجرائم المعلوماتية عبر الوطنية، لا تحدّها حدود خلافاً للجرائم التقليدية المعروفة، الأمر الذي يجعلها في كثير من الأحيان تستعصي على الخضوع للقوالب القانونية التي تحكم مسألة الاختصاص المكاني. ومن ثَم، فإن الطبيعة الخاصة لهذا الصنف من الجرائم المستحدَثة تتطلّب تجاوز القوالب والمعايير التي طرحها الفقه للتغلّب على مشكلة تنازع الاختصاص، والعمل على تبني حلول). ر مرونة تأخذ في الحسبان النطاق الجغرافي لهذه الجرائم وسهولة ارتكابها، وآلية اقترافها، والتخلص من آثارها وما إلى ذلك من اعتبارات يفرضها الطابع التقني المتطور لها، وهذا بطبيعة الحال، ينبغي ألاّ يُترك لمحض اجتهادات الفقه والقضاء، وإنما يلزم تدخل المشرّع لتحديد معايير الاختصاص التي يفترض عدم تضييق نطاقها، بحيث يكون من الملائم أن ينعقد الاختصاص لقانون أي بلد أضرت به الجريمة أو من المتوقّع أن

(1) Padovo (M.): La douane et la cyber - delinquance. G. P. 1996. Doctr. 1325.

(2) عرب، يونس، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، المرجع السابق.

تُشكل خطورة على مصالحه الحيوية، ولو كان مكان وقوعها خارج نطاق إقليمها. ومن المناسب بتقديرنا تبنّي مبدأ الاختصاص العالمي أو الشامل بهذا الخصوص من أجل تجنُّب الكثير من المشاكل الناجمة عن تحديد مكان وقوع الجريمة أو ترتب آثارها الضارة [1].

(1) عرب، يونس، قانون الكمبيوتر، موسوعة القانون وتقنية المعلومات، منشورات اتحاد المصارف العربية، الطبعة الأولى، الجزء الأول، 2001م.

المبحث التاسع

الاتجاهات الإقليمية والدولية ومشكلة الاختصاص

ونحن في الحاجة إلى أداء قانوني وقضائي عربي يُساير تحديات العصر الرقمي.

فقد أثارت البيئة الرقمية جملة من التحديات والمشكلات القانونية التي تطلبت وتتطلب تنظيماً قانونياً في جانب منها لعدم تعرُّض القوانين القائمة في الدول العربية لتنظيمها أو تتطلب إعادة تقييم للقواعد القائمة لتتواءم مع الطبيعة الخاصة لتطبيقات العصر الرقمي [1]، ومن أبرز التحديات القانونية في هذا الحقل تحديات التعاقد بالطرق الإليكترونية Contracting by Electronic Means، وتحديات وقانونية الدليل evidential value، وفي إطارها يظهر الموضوع الأهم، التواقيع الرقمية Digital Signature بجوانبه الموضعية والإجرائية، ويرتبط به موضوع التشفير Cryptography ويتصل بالإثبات مسالة الموقف القانوني من الرّسائل الإليكترونية Legal Recognition of Electronic Messages، وتحديات أنظمة الدفع الإليكتروني والمال الإليكتروني والبنوك الإليكترونية electronic money and electronic banking Payment systems، وتتصل هذه التحديات بمفهوم النقود الإليكترونية، الجوالات الإليكترونية، وآليات الدفع النقدي الإليكتروني. وتحديات المسئولية القانونية للجهات الوسيطة في أنشطة الخدمات والمنتجات الإليكترونية Liability of on-line intermediaries، ومسئولية جهات التوثيق وإصدار الشهادات Certificate authorities. وتحديات التنظيم القانوني للبنية التحتية Infrastructure، وتتعلّق بالتنظيم القانوني لخدمات الاتصال وتزويد خدمة الإنترنت وجهات الإشراف على الأعمال الإليكترونية في الدولة

---

(1) عرب، يونس، صور الجرائم الإليكترونية واتجاهاتها تبويبها ورقة عمل سنة 2006م.

المزودة لحلولها وروابطها، وما يتصل بهذا التنظيم من معايير ومواصفات وقواعد قانونية ومسئوليات قانونية. وتحديات حماية المستهلك وتنفيذ القانون Consumer protection and law enforcement وتحديات الملكية الفكرية Intellectual property في بيئة التجارة الإليكترونية، وتحديداً العلاقة بين حماية العلامات التجارية وأسماء النطاقات، إلى جانب حماية محتوى مواقع التجارة الإليكترونية من المواد المكتوبة والمرئية والمسموعة طبعاً إضافة إلى حماية برمجيات التجارة الإليكترونية وحلولها التقنية خاصة تلك التي يجري تنزيلها عن الموقع بصورة رقمية [1]. ومسائل أمن المعلومات IT Security المتصلة بأنماط اختراق مواقع التجارة الإليكترونية ونظمها ومتطلبات أمن الشبكات من مختلف صور جرائم الكمبيوتر والانترنت. وتحديات مسائل الخصوصية Privacy والضرائب Taxation والجمارك والتعريفة Customs وتنظيم مسائل التسليم المادي للمنتجات المنيعة على الخط: وتحديات الاختصاص والولاية القضائية Jurisdiction والقانون الواجب التطبيق Applicable Law، وتحديات فعالية النظام القضائي في هذه البيئة وأدواته الملائمة لضمان السرعة وسلامة المخرجات، أضف إلى ذلك كله، أن جوهر المشكلة ليس مجرد التشريع[2]، بل سلامة الإطار التشريعي وملاءمته من جهة، وآليات إنفاذه على نحو فاعل وملائم دون خلق معيقات أو ردود فعل سلبية من قبل المخاطبين بإحكام هذه القوانين كما حصل عربياً في حقل إنفاذ تشريعات الملكية الفكرية على قطاع البرمجيات، مع ما يستتبع ذلك من احتياجات البحث والدراسة والتدريب والتأهيل لكافة الجهات ذات العلاقة بالنظام القانوني والقضائي، وتطوير أدوات امتلاك المعرفة القانونية وتوظيف وسائل أتمتة المحتوى والحلول القانونية والقضائية (المعلوماتية القانونية).

---

(1) عرب، يونس، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، المرجع السابق.

(2) القدهي، مشعل عبدالله. (1422هـ). المواقع الإباحية على شبكة الانترنت وأثرها على الفرد والمجتمع. (1422/7/29هـ). http://www.minshawi.com/gadhi.htm

وأصبحنا الآن بصدد منازعات البيئة الرقمية وتحديات الاختصاص القضائي والقانون الواجب التطبيق يتوقع في البيئة الرقمية – وهو ما حصل فعلاً في الأعوام الخمسة المنصرمة – ظهور المنازعات بخصوص الإخلال بشروط التعاقد [1]، أو إلحاق الضرر بالغير أو الاعتداء على العلامات والأسماء التجارية للغير أو منازعات بخصوص تنفيذ العقد والتسليم المادي للبضائع، ومن الوجهة العملية وبتحليل الحالات القضائية التي نظرت أمام القضاء المقارن في أوروبا وأمريكا ظهر أن غالبية المنازعات تتصل بمسائل الملكية الفكرية ومسائل التعويض عن الضرر جراء المنتجات المعيبة أو الإخفاق في تقديم الخدمة بشكل صحيح [2].

ومشكلة منازعات التجارة الإليكترونية تكمن في أن الغالب في علاقاتها القانونية أنها تتم بين أطراف تختلف جنسياتهم وأماكن إقامتهم وتتعلّق بموقع لا يعلم مكانه ولا مكان الجهة التي تُديره ولا وموقع الخادم (السيرفر) الخاص به، كما أن القانون الواجب التطبيق أيضاً لا يكون محددا بوضوح[3]، وحتى في حال الاتفاق عليه بين المتعاقدين عبر العقد الإليكتروني تُثار مدى صحة مثل هذا الشرط في ضوء حقيقة أن المستخدم قد لا يكون قد قرأ العقد وهو بالتأكيد لم يناقشه وربما يقع هذا العقد وفق بعض النظم القانونية ضمن مفهوم عقد الإذعان، إضافة إلى أن ثمة العديد من النظم القانونية لا تتضمَّن للآن تشريعات منظمة لمسائل تقنية المعلومات، فما هو القانون الواجب التطبيق على منازعات التجارة الإليكترونية، ومن هي المحكمة المختصة، وما مدى حجية أحكام المحاكم الأجنبية ومدى قابليتها للتنفيذ في إقليم آخر، ثم ما هي أنجع الوسائل لفض منازعات التجارة الإليكترونية؟

---

(1) عرب، يونس، صور الجرائم الإليكترونية واتجاهاتها وتبويبها، المرجع السابق.

(2) الفيومي، محمد، «مقدمة في علم الحاسابات الإليكترونية والبرمجة بلغة بيسك»، المرجع السابق.

(3) عرب، يونس، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، المرجع السابق.

بالنسبة لأوروبا، حيث تسود النظم اللاتينية والجرمانية وكذلك الأنجلوسكسونية في بعض دولها [1]، أمكن لتجربة أوروبا الموحدة أن تُحقِّق التكامل الأوربي، ويقوم التكامل الأوروبي من الوجهة الاقتصادية على أربعة مبادئ، حرية انتقال البضائع، حرية انتقال الخدمات، حرية انتقال الأفراد حرية انتقال رؤوس الأموال، وما كان يمكن أن تكون هذه المبادئ فاعلة وحقيقة دون تحقيق تعاون واسع في حقلي الأحكام القانونية والتعاون القضائي، وقد حقَّقت اتفاقية بروكسل لعام 1968م حرية تبادل وانتقال القرارات القضائية، وقد أصبحت هذه الاتفاقية نافذة منذ عام 1988م بموجب اتفاقية لوجانو. وقد مثَّلت هذه الاتفاقية إضافة إلى اتفاقية روما لعام 1980م الخاصة بالقانون الواجب التطبيق على العقود والتي أصبحت نافذة عام 1990م، أحد ركائز تكامل الاتحاد الأوروبي [2].

إن القانون الأوروبي يجري تطويره عبر اتفاقيات بين الدول الأعضاء ومن خلال أنظمة ولوائح ومن خلال أدلة توجيهية وأوامر تشريعية أو تعليمات أيضاً، وتمثل المحكمة الأوروبية إطاراً هاماً لضمان التكامل والانسجام القانوني في الاتحاد الأوروبي، ومؤخراً، ضمن مسعى أوروبا لوضع حلول متكاملة لعصر الاقتصاد الرقمي، جرى تطوير القانون الأوروبي، ليتلاءم مع الآثار الجديدة لعصر المعلومات، وضمن هذا السياق، جرى وضع العديد من الأدلة التوجيهية والتعليمات التي استندت إلى دراسات شاملة ومتخصصة لكافة المسائل القانونية المتصلة بالتكنولوجيا والمعلومات، من ضمنها مسائل الاختصاص والقانون الواجب التطبيق في بيئة الانترنت، ولهذا خضعت اتفاقية بروكسل ولوجانو إلى مراجعة شاملة، وجرى تقديم مقترح وزاري للبرلمان الأوروبي لإجراء تعديلات على الاتفاقيات القائمة ومقترح التعديلات

---

(1) غاري، ج، بيتر، ثقافة الحاسوب، الوعي والتطبيق والبرمجة، الطبعة الأولى، ترجمة ونشر مؤسسة الأبحاث اللغوية، نيقوسيا، 1987م.

(2) Mohrenschlager (M): computer crimes and others crimes aganiste information technology in the Germany. Rev. Int. dr. pen. 1993, p 319, Spec. p 349.

لاتفاقية بروكسل المقدم من مجموعة العمل الوزارية [1]، جرى إقراره في عام 2000م، لا يمس القواعد والمبادئ الرئيسة لاتفاقية بروكسل، لكن التعديل يتصل بالمادتين 13 و14 من الاتفاقية، التي تنظم الاختصاص المتعلّق بعقود المستهلك، ووفق التعديل فإن محاكم الدول الأعضاء التي يُقيم ضمنها المستهلك تكون مختصة إذا وجه مورد البضاعة أو الخدمة (البائع) أنشطته إلى المنطقة التي يُقيم فيها المستهلك، وتكون أنشطة البائع موجَّهة لدولة المستهلك إذاً تحقيق التبادل المعلوماتي عبر الانترنت مع منطقة المستهلك.
كما صدر عن البرلمان الأوروبي وعن مجلس أوروبا في التطبيق، 98 تعليمات الأوامر القضائية المتعلّقة بحماية مصالح المستهلكين [2]، وحيث أن الأحكام القضائية والأوامر القضائية المتعلّقة بالإعلان والتسويق تتعلّق بالنظام العام وفقاً للقانون الدولي فإن هذه الأحكام والأوامر لن تكون قابلة للتنفيذ من قبل المحاكم الأجنبية، عوضاً عن عدم قدرة جمعيات ومنظمات حماية المستهلك التدخُّل فيما يتصل بالمستهلكين في دول أخرى غير الدول الموجودة فيها هذه المنظمات، وهذا سيؤدي إلى الإخلال بقواعد حماية المستهلك وإدخال المستهلكين في دائرة قانونية مفرغة، من هنا تبنّى البرلمان والمجلس هذه التعليمات أو الأمر التشريعي الذي تضمَّن أن محاكم الدولة العضو عليها أن تطبق الأحكام والأوامر القضائية الصادرة في دولة عضو أخرى، وهذا الحكم سيؤثر إيجاباً على أنشطة الاستثمار في بيئة الانترنت، باعتبار أن هيئات ومنظمات حماية المستهلك ستكون قادرة على التعامل مع الأنشطة الإعلامية والتسويقية وشروط البيع غير العادلة التي تتم من خارج الحدود. ولا يتضمَّن هذا التشريع حلولاً بشأن القانون الواجب التطبيق، وسيصبح نافذ اعتباراً من 31 كانون الأول 2000م. أما دليل الخدمات المالية فقد قدم

(1) ياسين، صباغ محمد محمد، الجهود الدولية والتشريعية لمكافحة الإرهاب وقرب العالم الجديد، دار الرضوان، القاهرة، 2005م.

(2) حجازي، سهير، التهديدات الإجرامية للتجارة الإليكترونية، مركز البحوث والدراسات، شرطة دبي بدولة الإمارات العربية المتحدة، 2005م.

للبرلمان الأوروبي ولمجلس أوروبا مشروع تعليمات المستهلكين المالية الخارجية، وهي تعليمات معدَّلة للتعليمات والأدلة التشريعية الخاصة بالخدمات المالية وتضمَّنت التعليمات المعدَّلة نصاً بخصوص الاختصاص وهو المادة 1/4/12أ وبموجبه يمكن للمستهلك أن يُقيم دعواه أمام محاكم إقامته أو محاكم إقامة البائع بغض النظر عن قواعد اتفاقية بروكسل[1]. أما الدعاوى المقامة على المستهلك فإنها محصورة بأماكن الدولة التي يوجد فيها مكان إقامته. وأما بالنسبة لتعليمات للتجارة الإليكترونية ففي أواخر عام 1998م تقدمت اللجنة الأوروبية بمشروع تعليمات أو أمر تشريعي خاص بالمسائل القانونية المتعلِّقة بالتجارة الإليكترونية (تعليمات التجارة الإليكترونية)، وقد أقرَّها البرلمان الأوروبي ومجلس أوروبا في 1998/11/18م، وتطبق على مزودي الخدمات المعلوماتية وتشمل كافة أنشطة التبدُّل والتحويل على الخط، كبيع البضائع على الخط، وتقديم الخدمات على الخط بأنواعها كالنشر الإليكتروني والخدمات المهنية والتسلية وغيرها، والتعريف غير مقتصر على التسليم الذي يتم على الخط، وإنما يشمل التسليم المادي للمنتجات المباعة على الخط. وفي حقل منازعات التجارة الإليكترونية فقد اعتمدت المادة 1/3 معيار أن الدولة المختصة بالنظر في النزاع هي دولة المنشأ الأصلي للخدمة، وهو معيار مختلف فيه بل إنه منتقد من منظمات حماية المستهلك وسيكون محل جدل لدى برلمانات الدول الأعضاء، وقد برَّرت اللجنة الأوروبية اختيار هذا المعيار لأنه يُتيح ويُشجع حرية انتقال وإقامة مشاريع الاستثمار المعلوماتي في أية دولة من دول الاتحاد وفيما بينها وفقاً لرأي اللجنة. وأن هذا المعيار يتعلَّق بالسلطات فقط كجمعيات حماية المستهلك ونحوها، وفيما يتعلَّق باختيار القانون الواجب التطبيق فإنه وفقاً لتعليمات البيع عن بعد[2]،

---

(1) الشافعي، محمد إبراهيم محمد، النقود الإليكترونية، مجلة الأمن والحياة، أكاديمية الشرطة، دبي، س 12، ع1، يناير، 2004م.

(2) عرب، يونس، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، المرجع السابق.

فإن المادة 2/12 (وكذلك المادة 3/11 من مشروع تعليمات الخدمات المالية المعدَّل) يُقر أن للدولة العضو أن تتَّخذ التدابير لتضمن أن المستهلك لن يفقد الحماية المقررة عند الاتفاق على القانون الواجب التطبيق عبر الاتفاقيات التعاقدية عندما تعين الاتفاقية قانون دولة غير الدول الأعضاء ليُطبق على العقد. وأن المستهلك لا يملك فقد حقوق مقررة له بموجب التعليمات، وبذلك قدمت هذه التعليمات ومشروع تعليمات الخدمات المالية حماية أكثر من تلك المقررة في المادة 5 من اتفاقية روما التي أقرَّت قانون إقامة المستهلك القانون الواجب التطبيق على العقد. وبالنسبة لمكان مواقع الانترنت فقد اقترح اعتبار موقع الانترنت أو سيرفر الانترنت بمثابة تأسيس (شركة) أو مؤسسة قائمة بالمفهوم المقرر في المادة 5/5 من اتفاقية بروكسل وصيغة لوجانو بشأن الاختصاص القضائي والمادة 2/4 من اتفاقية روما بشأن القانون الواجب التطبيق تعليمات التجارة الإليكترونية الأوروبية، أوضحت أن موقع الانترنت لا يمكن اعتباره كتأسيس شركة بمعنى أن الشركة لا يمكنها أن تتصرَّف على أنها منطقة تسويق (في نطاق دول الاتحاد الأوروبي إذا هي أنشأت سيرفر في إحدى دول الاتحاد الأوروبي، فالتأسيس القانوني والوجود القانوني يرتكز على مكان تنفيذ الأنشطة الاقتصادية الفعلية للموقع [1].

فالمحرِّك الرئيس لحل مشاكل الاختصاص والقانون الواجب التطبيق على منازعات التجارة الإليكترونية هي مسألة حماية المستهلك، وهي الأساس في تحديد الحلول والقواعد في هذا الحقل. ويظهر أيضاً أن التوجه الأوروبي فيه نوع من التناقض، إذ يختلف حل تعليمات التجارة الإليكترونية التي اعتمدت البلد الأصلي لمنشأ الخدمة، عن حلول التعليمات والأدلة التشريعية الأخرى ومقترَحات تعديل اتفاقية بروكسل وصيغة لوجارنو، التي تقوم على أساس النشاط المؤثر الموجَّه لمنطقة وجود المستهلك كمعيار عريض وأساسي

(1) القاسم، محمد بن عبد الله، والزهراني، رشيد، والسند، عبد الرحمن بن عبد الله، العمري، عاطف، تجارب الدول في مجال أحكام في المعلوماتية، مشروع الخطة الوطنية لتقنية المعلومات، 1423هـ.

.[1]

على أية حال فإن موردي الخدمات على الانترنت وأصحاب مشروعات الاستثمار المعلوماتي عليهم أن يُدركوا جيداً أن توجيه النشاط للمستهلكين الأوروبيين، يمكن أن تؤدي وفي الغالب إلى خضوعهم لاختصاص المحاكم الأوروبية وأن تُطبق عليهم القوانين الأوروبية المتشددة في نطاق حماية مستهلكيها، وأن الاعتراف بالقرارات الأجنبية وتطبيقها قد لا يكون متيسراً في نطاق الاتحاد الأوروبي إذا ما تعارض مع القواعد المشار إليها [2].

وبالرغم من وجود هذه الأدلة والاتفاقيات وتعديلاتها المقترَحة فإن نقصاً لا يزال قائماً في حقل منازعات التجارة الإليكترونية، لهذا مثلت الاتفاقية الصادرة عن مؤتمر هيوجو أواخر عام 2000م وسيلة هامة لسد النقص خاصة في حقل الاعتراف بالأحكام الأجنبية وإنفاذها في المسائل المدنية والتجارية.

أما بالنسبة للولايات المتحدة الأمريكية، فإنني قد تناولت تفصيلاً في موسوعة القانون وتقنية المعلومات - الكتاب الرابع منها بجزأيه - الجهود التشريعية المتَّخذة على المستوى الفدرالي لمواجهة مشكلات تنازع الاختصاص وتحديداً ما تضمَّنه قانون التجارة الأمريكي الموحَّد وقانون معلومات صفقات الحاسب لعام 1999م، وأما في حقل التطبيقات القضائية، فإن المحاكم الأمريكية التي نظرت عشرات المنازعات المتصلة بالانترنت أخضعت هذه المنازعات إلى ما يمكن تسميته فحص الاختصاص والولاية القضائية، ويعتمد فحص قابلية المحكمة لنظر الدعوى في القانون الأمريكي على توفر حد أدنى من الارتباط بين المدَّعى عليه ونطاق اختصاص المحكمة (مجتمع المحكمة) وهذا المعيار يختلف في فحص الاختصاص العام عنه في فحص الاختصاص

(1) حجازي، سهير، التهديدات الإجرامية للتجارة الإليكترونية، المرجع السابق.

(2) Digital Evidence and Computer Crime, by Eoghan Casey, 1st edition Academic Pr. 2000.

المحدَّد أو الخاص، ففي حقل الاختصاص العام (الفحص الأول عملياً) لا بد من وجود اتصال وارتباط منتظم بين المدعى عليه ومجتمع المحكمة وأما بشان الاختصاص الخاص أو المحدَّد عند انتفاء الاتصال المنتظم فإنه يتوقف على مدى وجود علاقة بين سلوك المدَّعى عليه وبين نطاق اختصاص المحكمة ومدى توجيه المدَّعى عليه أنشطته لمجتمع المحكمة إضافة إلى عوامل طبيعة الارتباط وعدد مرات الاتصال. وضمن هذه المعايير الموضحة تفصيلاً في ورقة العمل، كانت اتجاهات القضاء الأمريكي على النحو التالي [1]:

بالنسبة للمواقع التي يقتصر نشاطها على ممارسة الأنشطة الإعلانية للمنتجات والخدمات، إي أنها مجرد منصَّة إعلانية، والتي يُطلَق عليها مواقع، فقد قررت غالبية الأحكام القضائية الأمريكية عدم كفاية النشاط الإعلاني وعرض المعلومات فقط للقول بقيام الاختصاص لانتفاء التفاعل مع نطاق اختصاص المحكمة والمقيمين فيه، وسنُشير خلال المحاضرة لحالات تطبيقية في هذا الجانب عوضاً عما تناولته تفصيلاً في مؤلَّفنا المشار إليه. وحتى في الأحوال التي يظهر أن عدداً من الأشخاص المقيمين ضمن مجتمع المحكمة قد اتصل بهذا الموقع، فإن غالبية القرارات لم تجد في عدد الاتصالات مبرراً لوجود الاختصاص؛ لأن هذه المواقع لا تُوجِّه نشاطها خصيصاً لمجتمع المحكمة[2]، ومع هذا فقد صدرت بعض القرارات التي خالفت التوجُّه الغالب ووجدت أن الإعلان على موقع خاص بالمعلن وثبوت وجود نحو 300 دخول من قِبل مشتركين من مجتمع المحكمة يوفر الاختصاص للمحكمة باعتبار أن المعلَن لدى معرفته بحصول هذه الاتصالات قبل أن يضع نفسه في علاقة مع مجتمع المحكمة وقبل أن يخضع لقوانينها، وبغرض إعادة تقييم المحكمة العليا لاتجاه بعض المحاكم التي ترى في المواقع الإعلانية محلاً صالحاً لتحقيق

(1) Fighting Computer Crime: A New Framework for Protecting Information, by Donn B. Parker, 1 edition, John Wiley & Sons 1998.

(2) الحميد، محمد دباس، وماركوا ابراهيم نينو، حماية أنظمة المعلومات، دار الحامد، الطبعة الأولى، سنة 2007م.

الارتباط بمجتمع المحكمة بما يُبرر الاختصاص، قررت المحكمة فحصاً من خمسة معايير، يتضمَّن طبيعة الاتصال، عدد مرات الاتصال، نشوء سبب الدعوى عن الاتصال، مصلحة المجتمع في نظر الدعوى، مدى ملائمة المحكمة لنظر نزاع الأطراف [1].

أما بالنسبة للمواقع التي تُضيف إلى الإعلان أنشطة اتصالية أخرى، فإن المحاكم أصدرت قراراتها في ضوء طبيعة هذا الاتصال، فبالنسبة لإضافة وسيلة الاتصال الهاتفي المجاني للموقع، فقد اعتبرت المحاكم انه سلوك غير كافٍ لإقامة الارتباط بين المدَّعى عليه (مالك الموقع) والمحكمة لكنها قررت وجود ارتباط كافٍ فيما إذا مارس الموقع أنشطة إعلانية إليكترونية لمشتركين من مجتمع المحكمة، وكذلك في الأحوال التي ثبت فيها أن الموقع أنشأ قائمة بريد إليكتروني لمستخدميه تضمَّنت مشتركين من مجتمع المحكمة، وفي حالة ثبوت وجود مشتركين من نفس مجتمع المحكمة في خدمات صيانة وتطوير البرامج التي يعلن عنها [2].

وفيما يتعلَّق باختيار القانون الواجب التطبيق والشروط التعاقدية المتصلة بفض المنازعات، فإن إثارتها تم ضمن دعاوى تتعلَّق في الغالب برخص البرمجيات، ومدى مشروعية العقد الإليكتروني على الخط، ومدى قانونية التعاقد بمجرَّد الضغط على أيقونة (أنا أقبل)، وقد نما اتجاه قضائي نحو قبول هذه التعاقدات في الأحوال التي يثبت أن الموقع أتاح الفرصة للمستخدم لقراءة شروط العقد، وأن له خياراً متوفراً في الخروج من الموقع ورفض التعاقد، وقد قاست قبولها هذا على قبول القضاء لشروط رخص فض العبوة التي توضع مع حزمة البرنامج المباعة في الأسواق، إذ في الغالب لا يقرؤها

(1) عرب، يونس، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، المرجع السابق.

(2) اليوسف، عبدالله عبدالعزيز (1420هـ). التقنية والجرائم المستحدثة، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية، تونس، تونس (195 – 233).

الزبون لكن وجودها معه وإدراكه أن مجرد فض العبوة تجعله ملزماً بشروطها أدّى إلى قبول هذه الوسيلة التعاقدية [1]، في حين أن العقد الإليكتروني يوفر ضمانات أكثر للمستهلك من رخص فض العبوة. هذا مع الإشارة إلى أن قواعد حماية المستهلك تعمل جنباً إلى جنب مع هذا التوجُّه إذ في الحالات التي يظهر فيها احتمال عدم اطلاع المستهلك على الشروط بسبب عدم وضوحها، أو في الحالات التي لا يتضمَّن الموقع وسيلة إضافية لاحقة على قرار قبول التعاقد لتأكيده قضي بعدم صحة الشروط العقدية المقرَّرة للقانون الواجب التطبيق.

---

(1) عرب، يونس، جرائم الكمبيوتر والانترنت، موسوعة القانون وتقنية المعلومات، منشورات اتحاد المصارف العربية، الطبعة الأولى، الجزء الثاني، 2002م.



الفصل الخامس

التحقيق الجنائي و التفتيش في الجرائم المعلوماتية

القسم الأوَّل

التحقيق في الجرائم المعلوماتية

المبحث الأوَّل

مفهوم التحقيق الجنائي وعناصره في الجرائم المعلوماتية

المطلب الأوَّل

مفهوم التحقيق الجنائي

التحقيق الجنائي هو عملية تستدعيها المصلحة العامة، وتطبيق قواعد العدل والإنصاف بين أفراد المجتمع، لحماية آمن المجتمع وصوناً لاستقراره. من هنا، فهو يعني، في مفهومه العام، التحري والتدقيق في البحث عن شيء ما في سبيل التأكد من وجوده، أو السعي للكشف عن غموض واقعة معينة،

وينبغي لذلك استعمال طرق ووسائل محدَّدة يكفلها القانون لإجراء التحقيق.

المقصود بالتحقيق الجنائي من الناحية الاصطلاحية هو: تلمُّس السبل الموصلة لمعرفة الجاني في جناية ارتكبت أو شرع في ارتكابها، وكذلك ظروف ارتكابها، وذلك باستعمال وسائل مشروعة للتحقيق ومحدَّدة من جهة مختصة، أما من الناحية النظامية فإن عمليات التحقيق الجنائي وإجراءاته تقوم على أُسس وقواعد فنية يستخدمها المحقِّق بما كفله له النظام من سلطات، إذ يقوم بتنفيذ هٰذه الأسس والقواعد حتى يتسنى له بواسطتها الكشف عن غموض الجريمة، وتحديد مرتكبها، والوقوف على كل الأدلة الخاصة بها.

فمرحلة التحقيق تعتبر مرحلة مهمة قبل أن يتم النظر في الواقعة من قِبل المحكمة، وذلك لكونها من المراحل الإعدادية المهمة لتقديم قضية أو دعوى جنائية مكتملة للقضاء، ويعطي التحقيق الواقعة طابعها الرسمي من حيث اكتمال أدلتها، وتحديد مختلف جوانبها عند تقديمها، أو إحالتها للقاضي. وبذلك فإن عمليات التحقيق الجنائي هي المعنية لتحقيق واجب العدل والإنصاف والتحقُّق من براءة أو اتهام مقترِف الجريمة [1].

فالمحقِّق أو الباحث الجنائي هو الشخص الذي يتولى ويتكلَّف بالبحث وجمع الدلائل لكشف غموض الحوادث من قِبل رجال الضبط القضائي. وأضفنا بأن دور الباحث الجنائي يتحدَّد بالعمل على منع الجريمة قبل وقوعها، أو اكتشافها بعد وقوعها، وضبط مرتكبيها، والأدوات التي استُعملت فيها. ومن أهم واجباته في (مسرح الجريمة) أنه يعمل على عدم تضييع أي دليل من الأدلة الموجودة، أو العبث بها، أو الإهمال في المحافظة عليها.. تلاحظون أنني كرَّرت أكثر من مرة جملة «عدم تضييع أي دليل من الأدلة الموجودة، أو العبث بها، أو الإهمال في المحافظة عليها»، وسنُكررها لاحقاً، وذلك لأهميتها في التحري والبحث الجنائي.

---

(1) ممدوح، خالد فن التحقيق الجنائي في الجرائم الإليكترونية، دار الفكر الجامعي، 2009م.

المطلب الثاني

عناصر التحقيق في الجرائم المعلوماتية

يمكن تقسيم إجراءات التحقيق في الجرائم المعلوماتية كما أوردها بعض الفقهاء [1] إلى قسمين رئيسيين، قسم يهدُف إلى البحث عن الحقيقة سواء فيما يتعلّق بثبوت التهمة، أو عدم ثبوتها، أم سواء فيما يتعلّق بنسبتها إلى المتهم، وذلك بالبحث في الأدلة وتمحيصها، وهو ما يطلق عليه «إجراءات التحقيق» في معناها الدقيق، ويطلق عليها الفقه في مصر تعبير إجراءات جمع الأدلة، والقسم الثاني فلا يشمل إجراءات التحقيق بالمعني الدقيق لأنها لا تستهدف بحثاً عن أدلة، وإنما هي أوامر تحقيق تستهدف تأمين الأدلة من أسباب التأثير، أو العبث، ويطلق عليها الفقه «الإجراءات الاحتياطية ضد المتهم»، وهي الأمر بحضور متهم والأمر بالقبض عليه وإحضاره والأمر بحبسه احتياطياً، أما إجراءات التحقيق، فنقصد بها مجموعة الإجراءات التي تهدُف إلى التنقيب عن الحقيقة من حيث ثبوت التهمة ونسبتها إلى المتهم من عدمه، وأهم هذه الإجراءات هي التفتيش والانتقال والمعاينة وندب الخبراء وسماع الشهود والأستجواب. وتهدُف إجراءات التحقيق في الجزائم المعلوماتية إلى جمع وفحص الأدلة القائمة على وقوع الجريمة ونسبتها إلى فاعلها، وهي لم ترد في القانون على سبيل الحصر، بل يمكن مباشرة أي إجراء يفيد في كشف الحقيقة طالما أن المحقّق تقيَّد في مباشرته بحدود المشروعية. والمشرِّع المصري لم يُلزم المُحقق باتباع هذه الإجراءات وحدها دون غيرها في سبيل التنقيب عن الحقيقة، إذ يجوز للمحقّق أن يلجا إلى غير هذه الإجراءات طالما رأى أن فيها فائدة في كشف الحقيقة، ولم يكن في

---

(1) الصغير، جميل عبد الباقي، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، الطبعة الأولى، منشورات دار النهضة العربية، القاهرة، 1992م.

مباشرتها مساس بحرية المواطن أو بحرمة مسكنه، إلا أن القانون ألزم المُحقِّق بإجراء واحد هو استجواب المتهم [1].

وتتمثَّل تلك العناصر في التالي:

1 - الركن المادي للجرائم المعلوماتية:

إن النشاط أو السلوك المادي في جرائم المعلوماتية يتطلَّب وجود بيئة رقمية واتصال بالانترنت، ويتطلَّب أيضاً معرفة بداية هذا النشاط والشروع فيه ونتيجته، فمثلاً يقوم مرتكِب الجريمة بتجهيز الكمبيوتر لكي يتحقَّق له حدوث الجريمة، فيقوم بتحميل الكمبيوتر برامج اختراق، أو أن يقوم بإعداد هذه البرامج بنفسه، وكذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها مواد داعرة أو مخلَّة بالآداب العامة وتحميلها على الجهاز المضيف Hosting Server، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيداً لبثها[2].

لكن ليس كل جريمة تستلزم وجود أعمال تحضيرية في الحقيقة يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في نطاق الجرائم الإليكترونية، حتى ولو كان القانون لا يُعاقب على الأعمال التحضيرية، إلا أنه في مجال تكنولوجيا المعلومات الأمر يختلف بعض الشيء، فشراء برامج اختراق، وبرامج فيروسات، ومعدات لفك الشفرات وكلمات المرور، وحيازة صور دعارة للأطفال، فمثل هذه الأشياء تُمثِّل جريمة في حد ذاتها.

2 - الركن المعنوي للجرائم المعلوماتية:

الركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط بين

---

(1) أحمد، هلالي عبداللاه، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية (على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001م، الطبعة الأولى، دار النهضة العربية القاهرة، 2006م.

(2) رستم، هشام محمد فريد، الجرائم المعلوماتية (أصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي)، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت كلية الشريعة والقانون، بجامعة الإمارات العربية المتحدة، عام 2000م.

ماديات الجريمة وشخصية الجاني، وقد تنقَّل المشرِّع الأمريكي في تحديد الركن المعنوي للجريمة بين مبدأ الإرادة ومبدأ العلم، فهو تارة يستخدم الإرادة كما هو الشأن في قانون العلامات التجارية في القانون الفيدرالي الأمريكي، وأحياناً أخرى أخذ بالعلم كما في قانون مكافحة الاستنساخ الأمريكي[1].

3 - تحديد وقت ومكان ارتكاب الجريمة المعلوماتية:

تُثير مسألة النتيجة الإجرامية في جرائم المعلوماتية مشاكل عدة، فعلى سبيل المثال مكان وزمان تحقُّق النتيجة الإجرامية، فلو قام أحد المجرمين في أمريكا اللاتينية باختراق جهاز خادم Server أحد البنوك في الإمارات، وهذا الخادم موجود في الصين، فكيف يمكن معرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم، أم توقيت بلد البنك المسروق، أم توقيت الجهاز الخادم في الصين، وهذا بالتالي يُثير مشكلة أخرى، وهي مكان ارتكاب الجريمة المعلوماتية، ويثور أيضاً إشكاليات القانون الواجب التطبيق في هذا الشأن. حيث أن هناك بُعد دولي في هذا المجال، ذلك أن الجريمة المعلوماتية جريمة عابرة للحدود [2].

4 - علانية التحقيق:

علانية التحقيق من الضمانات اللازمة لتوافر العدالة، ولهذا قيل أن العلانية في مرحلة المحاكمة لا يقصر فيها الأمر على وضع الاطمئنان في قلب المتهم، بل إن فيها بذاتها حماية لأحكام القاضي من أن تكون محلاً للشك أو الخضوع تحت التأثير، كما أن فيها اطمئناناً للجمهور على أن الإجراءات تسير في طريق طبيعية. ولكن العلانية المقررة للتحقيق في الإجراءات الجنائية هي من بين الضمانات الخاصة به، وهي تختلف في التحقيق الابتدائي عنها في مرحلة المحاكمة. ففي التحقيق الابتدائي تُعتبر العلانية نسبية أي قاصرة على الخصوم في الدعوى الجنائية، والعلانية في التحقيق النهائي - أو

---

(1) إبراهيم، خالد ممدوح الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2009م.

(2) عرب، يونس، جرائم الكمبيوتر والانترنيت، المرجع السابق.

مرحلة المحاكمة – هي علانية مطلقة، بمعنى أنه يجوز لأي فرد من أفراد الجمهور الدخول إلى قاعة الجلسة وحضور المحاكمة [1].

والمشرِّع يُجيز في مرحلة التحقيق الابتدائي والتحقيق النهائي – مباشرة الإجراءات في غير علانية، فيصدر القرار بجعله سرياً، ولما كان هذا استثناء يأتي على قاعدة عامة أصلية كان من المنطقي أن نرى المشرِّع يُحدد الأحوال التي يجوز فيها جعل التحقيق سرياً، وهذه على كل حال رخصة لا يحسن الالتجاء إليها إلا عند الضرورة.

وإذا كانت الأمور التي تجري سراً من شأنها أن تولد الشك في القلب، وتبعث في النفس عدم الاطمئنان، فإن هذا الأثر كما يتحقَّق لدى المتهم، من الجائر أن يقوم في نفس الشاهد وأقواله من الأدلة الجنائية الهامة، ولهذا كان القرار بجعل التحقيق سرياً موجهاً للجمهور عامة وللشهود خاصة بأهمية وخطورة الواقعة التي يجري التحقيق فيها، وينعكس هذا الأثر في صورة اضطراب وتردد، بل قد يصل الأمر إلى إنكار المعلومات من جانب الشاهد [2].

---

(1) عريبه يونس، جرائم الكمبيوتر والانترنت، موسوعة القانون وتقنية المعلومات، منشورات اتحاد المصارف العربية، الطبعة الأولى، الجزء الثاني، 2002م.

(2) ممدوح، خالد فن التحقيق الجنائي في الجرائم الإليكترونية، المرجع السابق.

المبحث الثاني

معوقات التحقيق في الجرائم المعلوماتية

تتمثَّل عناصر التحقيق الجنائي في: إثبات وقوع الجريمة، وقت ارتكاب الجريمة، ومحل الجريمة، وأسلوب ارتكاب الجريمة، والباعث على ارتكاب الجريمة، الفاعل والشركاء والشهود إن وجدوا، ولا شك أن المعوِّقات تتمثَّل في كل مرحلة من هذه المراحل.

المطلب الأوَّل

صعوبات التحقيق في الجرائم المعلوماتية

يتَّسم التحقيق في الجرائم المعلوماتية وملاحقة مرتكبيها جنائياً بالعديد من المعوِّقات التي يمكن أن تُعرقل عملية التحقيق، بل يمكن أن تؤدي بها إلى الخروج بنتائج سلبية تنعكس على نفسية المحقِّق بفقدانه الثقة في نفسه وفي أدائه، وعلى المجتمع بفقدانه الثقة في أجهزة تنفيذ القانون غير قادرة على حمايته من هذه الجرائم وملاحقة مرتكبيها، وانعكاسها أيضاً على المجرم نفسه؛ حيث يشعر أن الجهات الأمنية غير قادرة على اكتشاف أمره وأن خبرة القائمين على المكافحة والتحقيق لا تُجاري خبرته وعلمه، الأمر الذي يعطيه ثقة كبيرة في ارتكابه المزيد من هذه الجرائم التي قد تكون أكثر فداحة، وأشد ضرراً على المجتمع المحلي، أو المجتمعات الأخرى [1].

(1) رستم، هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، 1994م.

الفرع الأوّل

صعوبات تتعلّق بالجريمة المعلوماتية ذاتها

1 - صعوبة الوصول إلى الدليل لإحاطته بوسائل الحماية الفنية كاستخدام كلمات السر حول مواقعهم تمنع الوصول إليها، أو ترميزها، أو تشفيرها؛ لإعاقة المحاولات الرامية إلى الوصول إليها، والاطلاع عليها، أو استنساخها.

2 - افتقاد أكثر آثار الجريمة التقليدية.

3 - خفاء الجريمة وغياب الدليل المرئي الممكن فهمه بالقراءة.

4 - أيضاً من المعوّقات المتعلّقة بالجريمة المعلوماتية سهولة محو الدليل، أو تدميره في زمن قصير جداً، ومن الأمثلة على ذلك قيام أحد مهرّبي الأسلحة في النمسا بإدخال تعديلات على الأوامر العادية لنظام تشغيل جهاز الحاسب الآلي الذي يستخدمه في تخزين عناوين عملائه والمتعاملين معه؛ بحيث يترتّب على إدخال أمر النسخ، أو الطباعة إلى هذا الحاسب من خلال لوحة مفاتيحه محو وتدمير كافة البيانات كاملة.

وفي واقعة مماثلة حدثت وقائعها بدولة الإمارات العربية المتحدة تتمثّل في قيام مشغّل حاسب آلي بتهديد المؤسسة التي يعمل بها لتنفيذ مجموعة من المطالب، وذلك بعد أن قام بحذف كافة البيانات من على الجهاز الرئيسي للشركة، وإزاء رفض المؤسسة الاستجابة لمطالبه أقدم على الانتحار مما سبب صعوبة بالغة في استرجاع البيانات التي كان قد حذفها.

فالجاني يمحو الأدلة التي تكون قائمة ضده أو تدميرها في زمن قصير جداً، بحيث لا تتمكن السلطات من كشف الجريمة إذا ما علمت بها، وفي

هذه الحالة التي قد تعلم بها، فإنه يستهدف بالمحو السريع عدم استطاعة هذه السلطات إقامة الدليل ضده، وبالتالي تنصُّله من مسئولية هذا الفعل وإرجاعه إلى خطأ في نظام الحاسب الآلي، أو الشبكة، أو في الأجهزة [1].

الفرع الثاني

صعوبات مرتبطة بالمجني عليه

1 - كما تُعد التقنية المستخدَمة في نظم المعلومات مجال استثمار ولذا تتسابق الشركات في تبسيط الإجراءات، وتسهيل استخدام البرامج والأجهزة وملحقاتها، وزيادة المنتجات واقتصار تركيزها على تقديم الخدمة، وعدم التركيز على الجانب الأمني، على سبيل المثال مستخدمو شبكة الانترنت عبر مزودي الخدمة وبطاقات الانترنت المدفوعة ليسوا مطالبين بتحديد هويتهم عند الاشتراك في خدمة الانترنت، أي أن مزوِّد الخدمة لا يعرف هوية مستخدم الخدمة.

2 - كما أن الإحجام عن الإبلاغ عن الأشخاص المسئولين بالمؤسسات خشية من المجتمع المحيط بهم، وخشية الفضيحة يُعد معوّقاً من معوّقات التحقيق، وقد يكون بهدف إخفاء الأسلوب الذي ارتُكبت به الجريمة؛ لكي لا يتم تقليده من الآخرين مستقبلاً.

3 - عدم إدراك خطورة الجرائم المعلوماتية من قِبل المسئولين بالمؤسسات تُعد إحدى معوّقات التحقيق.

(1) الصغير، جميل عبد الباقي، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، المرجع السابق.

4 - كما يُعد إغفال جانب التوعية لإرشاد المستخدمين إلى خطورتها معوّق آخر، وبالنظر إلى بعض المؤسسات نجد أنها أسست نظم معلوماتها على تطبيقات خاصة من التقنية على أساس أنها تُقدم لعملائها خدمات أسرع بدون عوائق، ويكون ذلك على حساب الأمن.

5 - كما يكون الإحجام عن الإبلاغ عن هذا النوع من الجرائم بسبب عدم رغبة الجهات المتضرِّرة في الظهور بمظهر مشين أمام الآخرين؛ لأن تلك الجرائم ارتُكبت ضدها، مما قد يترك انطباعاً بإهمالها، أو قلة خبرتها، أو عدم وعيها الأمني، ولم تتخذ الاحتياطات الأمنية اللازمة لحماية معلوماتها.

6 - ويكون الإفصاح عن التعرُّض لجريمة معلوماتية من شأنه حرمان شخص من خدمات معينة تتعلَّق بالنظام المعلوماتي، فقد يُحرم الموظف في الجهة من خدمات معينة على الانترنت، أو قد يُحرم من خدمات الانترنت عموماً حين يتعرَّض لجريمة معلوماتية ناتجة عن الاختراق، أو زيارته لأماكن غير مأمونة، أو غير مسموح بزيارتها، وقد يكون سبب عدم الإبلاغ عن الجريمة، عدم معرفة الضحية بوجود جريمة أصلاً، وعدم القناعة أنها ممكن أن تحدث في مؤسسته[1].

الفرع الثالث

صعوبات مرتبطة بالتحقيق

1 - تتعلَّق تلك الصعوبات بالنواحي الفنية، كنقص المهارة الفنية

(1) إبراهيم، خالد ممدوح، الجرائم المعلوماتية، المرجع السابق.

المطلوبة للتحقيق في هذا النوع من الجرائم، ونقص المهارة في استخدام الكمبيوتر والانترنت، وعدم توفر المعرفة بأساليب ارتكاب الجرائم المعلوماتية، وقلّة الخبرة في مجال التحقيق في جرائم الكمبيوتر والانترنت، والمعرفة باللغة الإنجليزية، سيما وأن للعاملين في مجال الكمبيوتر مصطلحات علمية خاصة أصبحت تُشكّل الطابع المميز لمحادثاتهم وأساليب التفاهم معهم [(1)].

2 - بعض هذه المعوّقات ترجع إلى شخصية المحقّق، مثل التهيُّب من استخدام جهاز الكمبيوتر، والتهيُّب من استخدام الانترنت، بالإضافة إلى عدم الاهتمام بمتابعة المستجدات في مجال الجرائم المعلوماتية.

وقد تكون أمام أجهزة الشرطة والنيابة مجالات متنوّعة ينبغي تغطيتها بالدعم والعناية، فهي ليست متفرّغة تماماً للجرائم المعلوماتية وحدها، ومن هنا كانت المناداة إلى إنشاء وحدة تحقيق خاصة بالجرائم المعلوماتية متفرّغة لهذا النوع من الجرائم، وقد يكون لحداثة هذا النوع من الجرائم وقلّة المستكشف منها سبب وراء عدم اكتساب تلك الأجهزة خبرة التعامل معها، ناهيك عن الانتشار الواسع للكمبيوتر وتنوُّع برامجه وأنظمته مما يجعل حصر أساليب الجريمة المعلوماتية وصورها وأنماطها صعباً، وبالتالي يتعذّر معه تدريب المحقّقين.

وعلى ذلك يرى البعض أنه من المستحسَن أن تُوكّل مهمة التحقيق في هذا النوع من الجرائم إلى بيوت الخبرة المتخصصة في هذا المجال لا سيما مع وجود شركات عالمية متخصصة في تحقيق الجرائم المعلوماتية حقّقت النجاح في كثير من الحالات.

---

(1) رستم، هشام محمد فريد، الجرائم المعلوماتية (أصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي)، المرجع السابق.

وجانب آخر يرى أن متطلّبات العدالة الجنائية تقتضي تحمُّل الأجهزة الأمنية الحكومية مسئوليتها تجاه اكتشاف كافة الجرائم، ومن بينها الجرائم المعلوماتية، وضبط الجناة فيها، وتحقيق العدالة في حقهم.

كما ينبغي على تلك الأجهزة تحمُّل توفير الإمكانيات التقنية اللازمة للتحقيق في الجرائم المعلوماتية، بالإضافة إلى الكوادر البشرية ذات الكفاءات المهنية المتخصصة في هذا المجال للاستعانة بها في التحقيق.

ومن الممكن وحتى تكتمل قدرات تلك الأجهزة في هذا المجال أن يتم الاستعانة بالنخبة المتخصصة في مجال الحاسب الآلي وتكنولوجيا المعلومات وكل ما يتعلّق بها في جميع مراحل الدعوى الجنائية بدءً من اكتشاف الجريمة المعلوماتية وانتهاءً بالتحقيق والمحاكمة [1].

ومن أجل ذلك، فإنه لا بد من إيجاد أسلوب خاص للتحقيق في هذه الجرائم أسلوب يجمع بين الخبرة الفنية والكفاءة المهنية، ومن الممكن حيال ذلك اتباع الخطوات التالية:

1 - تبادل المعلومات بين المحقّق وخبير الحاسب الآلي. وذلك قبل البدء في التحقيق، وأخذ أقوال الشهود والمشتبه فيهم، أو استجواب المتهمين، بحيث يشرح المحقّق للخبير أهمية ترتيب المتهمين والشهود، وطريقة توجيه الأسئلة إليهم.

ومن جهة أخرى يقوم الخبير بشرح الأبعاد الفنية والنقاط التي ينبغي استجلائها من الأشخاص، وكافة المصطلحات الحاسبية التي يمكن استخدامها، مع بيان معانيها؛ ليتم الاستفادة منها عند الضرورة.

---

1) أحمد هلالي عبد اللاه، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية (على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001م، الطبعة الأولى، دار النهضة العربية القاهرة، 2006م.

2 - يتم أخذ أقوال الشهود، واستجواب المتهمين من قبل المحقّق، وبحضور الخبير الذي يجوز له توجيه الأسئلة الفرعية أثناء الاستجواب وفق الكيفية التي يتم الاتفاق عليها مسبقاً قبل بدء التحقيق.

3 - يتم حصر النقاط المطلوب استجلائها من قبل الخبير والمحقّق قبل البدء في التحقيق؛ ليتولى المحقّق بعد ذلك ترتيب تلك النقاط.

4 - التعاون بين المحقّق والخبير في الحصول على البيانات المخزّنة في الحاسب الآلي وملحقاته الخاصة بالشاهد أو المتهم الذي تم التحقيق معه. مع مراعاة أن هذا الأخير لا يجوز إجباره على تقديم دليل يُدينه.

ولضمان نجاح التحقيق في الجرائم المعلوماتية، فهناك بعض القواعد التي ينبغي مراعاتها أهمها [1]:

1 - تفادي ضياع الوقت في التحقيق حول جرائم لا يمكن اكتشافها، أو أن الأدلة اللازمة لاكتشافها وإثبات التهمة قد قُضي عليها.

2 - ضرورة مراعاة وجود نوع من التعامل بين المحقّقين وخبراء الحاسب الآلي العاملين في المؤسسة المجني عليها.

3 - مراعاة القوانين السارية بشأن الحقوق الفردية وسرية البريد الإليكتروني وغيرها من الحقوق.

4 - العناية بإصدار الأوامر القضائية الخاصة بالتفتيش وضبط أجهزة الحاسب الآلي، وملحقاتها، وبرامجها.

5 - مراعاة حفظ الأدلة الجنائية بالطرق المناسبة كل حالة على حده

(1) بلال، أحمد عوض، قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة، دار النهضة العربية، القاهرة، 1994م.

، وذلك حتى يتم تقديمها للمحكمة وهي على حالتها التي ضُبطت عليها .

6 - الاستعانة بالتقنيات المتطورة في المجال المعلوماتي في مواجهة الجرائم المعلوماتية، سيما وأن هذه التقنيات أثبتت جدارتها ونجاحها في جمع الأدلة الجنائية، وصناعة البنية الاتهامية، وتحليل القرائن، واستنتاج الحقائق.

الفرع الرابع

صعوبات مرتبطة بالدليل الإليكتروني

الضابط المحقّق في مثل تلك الجرائم يتمثّل في اعتبارات المعرفة الأساسية لكل من الضباط والمحقّقين لمفهوم الجرائم المعلوماتية، وهل ما قام به يُعد جريمة في قانون الدولة التي ينتمون إليها من عدمه، وكذا قانون الدولة المتواجد بها المشتبه فيه الأمر الذي تنشأ عن مشكله آخرى، وهو كيفية الحصول على الدليل عبر الحدود، وربما يكون ذلك الدليل غير قائم بالفعل، وكيفية اكتشاف الجريمة الطريقة التي تكتشف بها الجرائم.

وغالباً ما يحدث خلل وظيفي ما في الأجهزة، أو المواقع الخاصة لموفري الخدمات ينتج عن ذلك الخلل الصحفي والتحقيق، ويتم بعد ذلك اكتشاف الجريمة، الأمر الذي يجد معه أن يكون لدى أعضاء النيابة الكافية لمعرفة البدء في التحقيقات، وهذا ما نُطلق عليه عبارة: «الوضع المناسب والإشارة الصحيحة»، فإذا لم تُحدَّد الجريمة، ولم يتم التحفظ على الدليل، فإن الأثر المباشر لهذا هو عدم وجود الجريمة [1].

---

(1) الصغير، جميل عبد الباقي، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، المرجع السابق.

ومن ثم يجب على أعضاء النيابة والضابط منذ فجر تفشّي نبأ الجريمة الحفاظ على الدليل وتقنيته بالطرق المبيِّنة سلفاً؛ وذلك لأن الدليل الإليكتروني سهل التغير، ويكون ذلك بالتعاون مع الجهات التي تُقدم الخدمة بإجبارهم بوسيلة ما في الحفاظ على الدليل وعدم البعثرة فيه، وأن يتم تعيين بعض من المتخصصين تخول لهم سلطة الضبط والتفتيش في تتبع الدليل.

كذلك فإن هناك معوّقات كثيرة قد تعترض الحصول على الأدلة بالنسبة للجرائم التي تُرتكب بالوسائل الإليكترونية، ومثال ذلك أنه قد يتعذّر اتخاذ إجراءات التفتيش لضبط هذه الجرائم عندما يكون الحاسب الآلي متصلاً بحاسبات أخرى خارج الدولة، ويكون تفتيش هذه الحاسبات ضرورية لإماطة اللثام عما تشتمله من جرائم.

وليس بخافٍ علينا أن الجرائم التي تُرتَكب في فضاء شبكة الانترنت كما أنها تقع على المستوى الوطني، فإنها قد تُرتَكب أيضاً على المستوى الدولي، وهذا يُثير مشكلات عديدة مثل تتبع الاتصالات الإليكترونية عن طرق سلطات التحقيق لأجل إقامة الدليل على الجرائم التي تُرتَكب في مجال الانترنت [1].

ولا شك في أن اختلاف التشريعات فيما بينها فيما يتعلّق بشروط قبولها للأدلة وتنفيذ بعض الإجراءات اللازمة لضبط هذا النوع من الجرائم العابرة للحدود، فعلى الرغم من أن إرهاصات الثورة التكنولوجية في مجال الاتصال عن بعد قد أفرزت العديد من الجرائم ذات الطبيعة الخاصة، فما زالت إجراءات البحث عن هذه الجرائم وضبطها تتم في إطار النصوص الإجرائية التقليدية التي وُضعت لكي تُطبق على الجرائم التقليدية التي تنص عليها القوانين العقابية، الأمر الذي سيترتّب عليه الكثير من المشكلات بالنسبة لضبط هذه الجرائم المعلوماتية ذات الكيان المعنوي، والتي قد تتعدد أماكن ارتكابها داخل الدولة الواحدة، أو يمتد نطاقها ليشمل الكثير من

(1) أحمد، هلالي عبد اللاه، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، المرجع السابق.

الدول عبر شبكة الانترنت، كما هو الحال في شأن جريمة غسيل الأموال عبر الانترنت، فيتعذَّر تبعاً لذلك اتخاذ إجراءات جمع الدليل بالنسبة لها، أو قد تلحق عدم المشروعية بهذه الإجراءات [1].

ولذلك نجد أن بعض الفقه في ألمانيا يُشكِّك في إمكانية الدخول إلى أنظمة تقنية المعلومات لدى الحاسبات الأخرى التي توجد بالخارج؛ بغرض ضبط البيانات المخزَّنة بها؛ لأنه بدون وجود اتفاق بين الدول المعينة ينظم ذلك، فإن اتخاذ مثل هذا الإجراء يُعد خرقاً لسيادة كل دولة على إقليمها، ويُخالف الاتفاقيات الثنائية الخاصة بإمكانية التعاون في مجال العدالة القضائية. ويُلاحظ في هذا المجال تصادم التفتيش عن الأدلة في الجرائم المعلوماتية مع الحق في الخصوصية المعلوماتية، وذلك لأن هذا التفتيش يتم - غالباً - على نظم الكمبيوتر وقواعد البيانات وشبكات المعلومات، الأمر الذي قد يتجاوز النظام المعلوماتي المشتَبه به إلى أنظمة أخرى مرتبطة، نظراً لشيوع التشبيك بين الحاسبات، وانتشار الشبكات الداخلية على مستوى المنشآت والشبكات المحلية والإقليمية والدولية على مستوى الدول، ولا شك في أن امتداد التفتيش إلى نظم غير النظام محل الاشتباه قد يمس - في الصميم - حقوق الخصوصية المعلوماتية لأصحاب النظم المعلوماتية التي يمتد إليها التفتيش [2].

الفرع الخامس

الأخطاء المتعلِّقة بالتحقيق الجنائي

هناك أخطاء شائعة في التحقيق التحقيق، بعضها متعلِّقة بكيفية تدوين

(1) البشري، محمد الأمين، الأدلة الجنائية الرقمية، مفهومها ودورها في الإثبات، المجلة العربية للدراسات الأمنية والتدريب، المجلد 17، العدد 33، السنة 17، الرياض، إبريل 2002م.

(2) قايد، أسامة عبد الله، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، المرجع السابق.

التحقيق، والأخيرة يرد إلى تصرُّفات المُحقِّق ذاته، ونذكر غالبية هذه الأخطاء حتى يمكن تفاديها وتلافيها، ونذكرها على النحو التالي:

أوّلاً: أخطاء شائعة متعلِّقة بكيفية تدوين التحقيق:

هناك العديد من الأخطاء الشائعة البارزة في مجال تدوين التحقيق نذكر أهمها على النحو التالي:

1 - عدم قيام عضو النيابة المُحقِّق بإثبات الميعادالحقيقي لورود المحضر لمقر النيابة المختصة، وقد يكون ذلك بغرض مجاملة ضابط الشرطة محرر المحضر، حيث يُثبت ساعة وتاريخ ورود المحضر، على خلاف الحقيقة، قبل ميعاد عرض المحضر فعلياً على وكيل النيابة بغية تجنب سقوط حجز المتهم لانتهاء المدة القانونية، أو لانتهاء الفترة المحددة في إذن النيابة لتنفيذه.

2 - اعتماد عضو النيابة العامة على الموظف سكرتير النيابة في تدوين أسماء المتهمين أو الشهود في المحضر، وأحياناً توجيه بعض الأسئلة والإجابة عليها، دون الإشراف عليه اعتماداً على خبرته الطويلة في العمل.

وكذلك الحال بالنسبة لمأمور الضبط القضائي؛ حيث يعتمد على بعض مساعديه أو معاونيه، كأمناء الشرطة مثلاً، في تحرير المحاضر الهامة بأسمائهم، الأمر الذي يؤدي إلى حدوث أخطاء جسيمة سواء فيما يتعلَّق بصحة الإجـراءات، أو فيما يتعلَّق بتدوين إجابات المستجوبين، وما يوجهه من أسئلة مثل إغفال جوانب هامة في الواقعة كإغفال تاريخ تحرير المحضر، أو ساعة افتتاحه؛ لذا ينبغي أن تتم كافة إجراءات التحقيق بمعرفة المُحقِّق

وتحت إشرافه الفعلي [1].

أما بالنسبة لضابط الشرطة متلقّي البلاغ فقد يقوم، مثلاً: بإثبات ميعاد غير حقيقي للبلاغ؛ وذلك لإعطاء نفسه فرصة للحصول على اعتراف المتهم حتى يتمكن من عرضه على النيابة خلال فترة 24 ساعة مما يؤدي إلى إصابة التحقيق في مقتل، وخاصة إذا لم يتلائم التاريخ والساعة مع الوقائع المدونة بالتحقيق، ومن شأن ذلك عدم اطمئنان المحكمة المختصة بنظر الموضوع للواقعة وإبراء ساحة المتهم [2].

3 - الإهمال في مناظرة، ووصف المضبوطات بدقة وإهمال تحريزها، الأمر الذي من شأنه التشكيك فيها وإعطاء ذوي النفوس الضعيفة والأمّارة بالسوء من التغير فيها أو تبديلها، ومن شأن ذلك فقدان الدليل لأهميته وعدم إسناد الواقعة للمتهم إسناداً صحيحاً.

لذا نؤكّد على أهمية قيام المُحقّق بوصف الحرز وصفاً دقيقاً، وله أن يستعين في ذلك بما شاء من أهل الخبرة، وأن يقوم بتحريزه بنفسه، أو تحت إشرافه الفعلي الحقيقي.

4 - قد يعمد عضو النيابة إلى تغيير الوصف القانوني للواقعة، كأن تكون سرقة بالإكراه، أو سرقة مشدّدة لوجود ظرف الليل، فيعتمد إلى وصفها بالسرقة البسيطة.

5 - قد يعمد عضو النيابة المُحقّق إلى إضافة أقوال، أو تحشير بعض الكلمات، أو إزالة بعضها، أو الكشط، بغرض توجيه مجرى

(1) رستم، هشام محمد فريد، الجرائم المعلوماتية (أصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي)، المرجع السابق.

(2) مراد، عبد الفتاح، شرح التحيق الجنائي الفني والبحث الجنائي، دار الكتب والوثائق المصرية، القاهرة 2000م.

التحقيق في اتجاه محدَّد، الأمر الذي يُشكِّك في صحة ما دوَّنه بمحضر التحقيق، كما أن تلك الواقعة، لو صحَّت، تُشكِّل جناية تزوير.

الفرع السادس

الأخطاء المتعلِّقة بتصرفات المُحقِّق

1 - البطء في الانتقال لمكان وقوع الجريمة لمعاينته، الأمر الذي قد يؤدي إلى طمس معالم الجريمة وآثارها التي تركها الجاني، وانصراف الشهود المتردِّدين بصفة مؤقتة وتصادف وجودهم وقت حدوث الواقعة [1].

2 - الميل إلى إيحاء أو تلميح بأقوال معينة يُبديها الشاهد، أو المجني عليه، أو المتهم للتخفيف من الواقعة، أو إقامة التهمة قبل شخص معين دون غيره، أو ينفيها أو يؤكِّدها، الأمر الذي يؤدي إلى تعرُّض التحقيق لمطاعن الدفاع.

3 - تشبث عضو النيابة المُحقِّق برأي واتجاه معين في كشف الجريمة وإهماله لكافة الاتجاهات الأخرى المحتملة، وتأثر المحقِّق بما يُبديه أحد الأطراف في الخصومة من أقوال دون الاستماع إلى الطرف الأوَّل، الأمر الذي قد يظهره أمام الأخير بمنظر المنحاز وغير عادل مما يؤثر على اتجاهاته في التحقيق وما يتَّخذه من إجراءات.

4 - البطء في إخطار خبراء الطب الشرعي، أو خبراء الأدلة الجنائية

---

(1) رستم، هشام محمد فريد، الجرائم المعلوماتية (أصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي)، المرجع السابق.

مما يؤدي إلى تأخُّر انتقالهم، الأمر الذي من شأنه أن يؤدي إلى حدوث تغيير في الآثار وطبيعتها مما يصعب من صلاحيتها لرفعها من مسرح الجريمة، وبالتالي معالجتها لاستخراج النتائج منها.

القسم الثاني

التفتيش في الجرائم المعلوماتية

مقدمة:

يُعتبر التفتيش من أخطر الحقوق التي مُنحت للمحقِّق، وذلك لمساسها بالحريات التي تكفلها الدساتير في شتى الدول؛ ولذا نجد المشرِّع يضع لها ضوابط عديدة سواء فيما يتعلَّق بالسلطة التي تُباشر أو تأذن بمباشرته، والأحوال التي تجوز فيها مباشرته، وشروط اتخاذ هذا الإجراء بما يُمثِّل ضمانات الحرية الفردية أو حرمة المسكن.

أن الأنظمة الجنائية عرفت في مراحل تطوّرها أنواعاً من الإجراءات تنطوي على انتهاك لحقوق الفرد الأولية في سبيل تتبع الجناة ومحاكمتهم ،ومنها القبض والتفتيش، فإذا ما تخلَّت يد العدالة عن التعرُّض لحقوق الأفراد لأصبحنا إزاء فوضى إجرامية، ومن ثم يجب أن يُتاح للقائمين على تنفيذ القانون نوع من السلطة في إنكار الحريات الشخصية بالقدر الذي يحول دون تسلُّط الإجرام على مقدَّرات الناس، وإنما لا ينبغي أن يتجاوز هذا القدر، إذ لا فارق بين أن تنتهك حريات الأفراد بمعرفة أشخاص يعملون تحت ستار القانون، أو بمعرفة مجرمين يرتكبون آثامهم بمنأى عن سطوة القانون ،ومن هذه الإجراءات التفتيش [1].

ومن أخطر الإجراءات التي يجريها مأمور الضبط القضائي في إثباته للجريمة إجراءات التفتيش سواء ما تعلَّق بشخص المتهم، أو مسكنه؛ لأنه ماس بحريته وسكينته، ولخطورة ما يُسفر عنه من أدلة تكشف وجه الحقيقة، وقد حرص الدستور الدائم في جمهورية مصر العربية على تقرير حرمة الأشخاص والمساكن وجعلها مصونة لا يجوز المساس بها إلا بأمر قضائي مُسبب، أو في حالة تلبُّس.

---

(1) الطوالبه، علي حسن، التفتيش الجنائي على نظم الحاسوب والانترنت – دراسة مقارنة، ط1، عالم الكتب الحديث، اربد، 2004م.

المبحث الأوّل

مفهوم وموضوع ومحل التفتيش

المطلب الأوّل

مفهوم التفتيش

يُعرَّف التفتيش بوجهٍ عام بأنه عبارة عن: «إجراء من إجراءات التحقيق التي تهدُف إلى البحث عن أدلة مادية لجناية أو جنحة تُحقِّق وقوعها في محل يتمتع بحرمة المسكن أو الشخص، وذلك بهدف إثبات ارتكابها، أو نسبتها إلى المتهم وفقاً لإجراءات قانونية محدَّدة»[1].

والتفتيش عمل قضائي لا يجوز أن يقوم به إلا من خوله القانون صفة الضبطية القضائية.

وعرَّفه البعض بأنه: «البحث عن الأشياء المتعلِّقة بالجريمة لضبطها ،وكل ما يُفيد في كشف حقيقتها، ويجب أن يكون للتفتيش سند من القانون». وعرَّفه آخرون بأنه هو: «البحث عن الحقيقة في مستودع سرها حيثما تكون مع الشخص، أو في منزل الحقيقة التي تتمثَّل في ثبوت أو انتفاء ارتكاب شخص معين لجريمة معينة وقعت بالفعل، واتهم هذا الشخص بارتكابها على أساس من الجدية التي تؤيدها إمارات قوية» [2].

ونخلص مما سبق أن المقصود بالتفتيش القانوني هو:

---

(1) الطوالبه، على حسن، مشروعية الدليل الإليكتروني المستمد من التفتيش الجنائي، «دراسة مقارنة الحقوق جامعة العلوم التطبيقية، البحرين، 2005م.

(2) أحمد، هلالي عبد اللاه، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دراسة مقارنة، ط1، دار النهضة العربية، القاهرة، 1997م.

-الذي ينصرف على تفتيش الشخص أو المسكن، وبالتالي تفتيش المحال العامة، والتفتيش في تلك الحالة يُعد إجراء إداري.

- التفتيش عملاً إجراء من إجراءات التحقيق أي لا بد من وقوع جريمة وأن يؤدي إلى التوصُّل لحقيقتها وفاعلها.

وتكمن الفكرة الأساسية للتفتيش في إباحة انتهاك الحق في الخصوصية طالما أن هناك مبرراً في القانون لهذا الانتهاك؛ لذا فهو يُعد من بين أقصى الصلاحيات التي قد تُمارسها الدولة ضد المواطن، ويُعد أحد مظاهر تقييد الحريات الإنسانية التي ساهمت التشريعات الكبرى الأساسية في دعم المحافظة عليها.

والغاية من التفتيش هي البحث عن الأشياء المتعلِّقة بالجريمة الجاري جمع الاستدلالات أو حصول التحقيق بشأنها، وكما تذهب محكمة النقض يكون التفتيش بمناسبة جريمة وقعت وأسند ارتكابها إلى شخص معين، وتقوم دلائل كافية على ارتكابه لها بما يُبرر انتهاك حرمة المحل الذي منحه القانون حرمة خاصة.

المطلب الثاني

موضوع التفتيش في الجريمة المعلوماتية

إذا كانت الجريمة واقعة على المكوّنات المادية للكمبيوتر، فلا عائق يحول دون تطبيق القواعد التقليدية للتفتيش، أما إذا كانت الجريمة واقعة على برامج الكمبيوتر وبياناته، فإن الصعوبات تبرز على اعتبار أن بإمكان الجاني التخلُّص من البيانات التي يستهدفها التفتيش عبر إرسالها من خلال نظام معلوماتي من مكان إلى آخر، أو إلى نظام معلوماتي آخر، وعلى اعتبار

أن التفتيش عن هذه البيانات يستوجب الكشف عن الرقم السري pass ward للمرور إلى ملفات البيانات، وهذا الرقم السري يعرفه المتهم، ولا يمكن إجباره على البوح به أو الإفصاح عنه [1].

ومن أجل تخطّي هذه الصعوبات، يجب أن لا يكون الإذن بالتفتيش محدَّداً بمكان معين، بل يجب أن يمتد إلى تفتيش أي نظام آلي موجود في مكان آخر بهدف التوصُّل إلى بيانات يمكن أن تُفيد بشكل معقول في كشف الحقيقة، شرط عدم انتهاك سيادة دولة أخرى، وأن يحل قاضي التحقيق محل الشخص صاحب المكان المراد تفتيشه بصورة مؤقَّتة.

كما يجب أن يتضمَّن إذن التفتيش الإجازة بالبحث عن كيان البرنامج ،وأنظمة تشغيله، والسجلات التي تُثبت استخدام الأنظمة الآلية لمعالجة البيانات والسجلات المستخدَمة في عملية الولوج في النظام الآلي لمعالجة البيانات.

المطلب الثالث

محل التفتيش في الجرائم المعلوماتية

إن تفتيش نظم الحاسب تفتيش للفضاء الافتراضي، وأوعية التخزين وتفتيش للبيانات التي يحفظها جهاز الكمبيوتر إن كان مزوداً بحافظات إليكترونية للعمليات المنجَزة من خلاله، وهو أمر يتعلَّق بالقدرة على تحديد المطلوب مسبقاً، وليس مجرد سبر غور نظام معلومات إليكتروني؛ لأن التعامل وفق المسلك الأخير قد يكون له عواقب قانونية أهمها بطلان الإجراءات

(1) الطوالبه، علي حسن، مشروعية الدليل الإليكتروني المستمد من التفتيش الجنائي، دراسة مقارنة، المرجع السابق.

لأنها خارج نطاق أمر التفتيش والضبط، أو قد تنطوي الإجراءات على كشف خصوصية البيانات المخزَّنة في النظام.

والدخول غير المشروع إلى الأنظمة المعلوماتية للبحث والتنقيب في البرامج المستخدَمة، أو في ملفات البيانات المخزَّنة عما قد يتصل بجريمة وقعت، إجراء يُفيد في كشف الحقيقة عنها وعن مرتكبها، وتقتضيه مصلحة وظروف التحقيق في الجرائم المعلوماتية، وهو إجراء جائز قانوناً ولو لم ينص عليه صراحة باعتباره يدخل في نطاق التفتيش بمعناه القانوني ويندرج تحت مفهومه [1].

ومحل التفتيش في الجرائم المعلوماتية (الوعاء الإليكتروني) هو جهاز الكمبيوتر والأجهزة المتصلة به، والشبكة التي تشمل في مكوّناتها مقدم الخدمة، والمزود الآلي، والمضيف، والملحقات التقنية، وهذا يعني أن التفتيش سوف ينصب على المكوّنات الآتية:

1 - مكوّنات مادية Hardware، وأخرى منطقية Software، أو ما يصطلح على تسميته بالقطع الصلبة والبرمجيات.

2 - شبكات اتصال بعدية Networks Telecommunication سلكية ولاسلكية محلية ودولية.

ويمكن أن يشمل تفتيش نظم الوسائل الإليكترونية كل مكوّناتها المادية والمعنوية على النحو سالف الإشارة إليه. ويمكن أن يشمل التفتيش أيضاً شبكات الاتصال الخاصة بها، والأشخاص الذين يستخدمون هذه الوسائل، وتتكوّن المكونات المادية لهذه الوسائل من وحدة المدخلات، ووحدة الذاكرة الرئيسة، ووحدة الحساب والمنطق، ووحدة التحكم، ووحدة المخرجات، ووحدات التخزين الثانوية، وأما المكوّنات المعنوية فهي عبارة عن برامج النظام وبرامج التطبيقات.

---

(1) إبراهيم، خالد ممدوح الجرائم المعلوماتية، المرجع السابق.

ويُضاف إلى ذلك أن الوسائل الإليكترونية بمكوّناتها المختلفة تستلزم لتشغيلها وجود مجموعة من الأشخاص أصحاب الخبرة والتخصص في مجال تقنية المعلومات، وهم مشغلوا الحاسب، خبراء البرمجة سواء كانوا مخططي برامج تطبيقات أم مخططي برامج نظم، والمحلّلين ومهندسي الصيانة والاتصالات، ومديري النظم المعلوماتية [1].

الفرع الأوّل

تفتيش المكوّنات المادية لجهاز الكمبيوتر

ليس هناك خلاف على أن الولوج إلى المكوّنات المادية للكمبيوتر بحثاً عن شيء ما يتّصل بجريمة معلوماتية الكمبيوتر، في كشف الحقيقة عنها وعن مرتكبها يخضع للإجراءات القانونية الخاصة بالتفتيش، بمعنى أن حكم تفتيش تلك المكوّنات المادية يتوقّف على طبيعة المكان الموجودة فيه تلك المكوّنات، وهل هو من الأماكن العامة أو من الأماكن الخاصة؛ حيث أن صفة المكان وطبيعته أهمية قصوى خاصة في مجال التفتيش، فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكمة، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه، وبنفس الضمانات والإجراءات المقررة قانوناً في التشريعات المختلفة، مع مراعاة التمييز بين ما إذا كانت مكوّنات الكمبيوتر المراد تفتيشها منعزلة عن غيرها من أجهزة الكمبيوتر الأخرى، أم أنها متصلة بكمبيوتر آخر أو بنهاية طرفية Terminal في مكان آخر كمسكن غير المتهم مثلاً، فإذا كانت كذلك وكانت هناك بيانات مخزّنة في أوعية هذا النظام الأخير من شأنها كشف الحقيقة تعين مراعاة القيود والضمانات التي يستلزمها المشرّع لتفتيش هذه الأماكن، ولو وجد

---

(1) أحمد، هلالي عبد اللاه، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق.

شخص يحمل مكوّنات الكمبيوتر المادية، أو كان مسيطراً عليها، أو حائزاً لها في مكان ما من الأماكن العامة سواء أكانت عامة بطبيعتها كالطرق العامة والميادين والشوارع، أو كانت من الأماكن العامة بالتخصيص كالمقاهي والمطاعم والسيارات العامة، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا المجال [1].

وإذا كانت تلك المكوّنات في حوزة شخص سواء أكان مبرمجاً، أو عامل صيانة، أو موظفاً في شركة تنتج برامج الكمبيوتر، إذ تنطبق حينئذٍ نفس أحكام تفتيش الأشخاص، وبنفس الضمانات والقيود المنصوص عليها في هذا المجال.

وهناك قلّة من التشريعات تنص صراحة على تفتيش مكوّنات جهاز الكمبيوتر منها على سبيل المثال قانون إساءة استخدام الكمبيوتر الإنجليزي الصادر في 1990/6/29م، وهناك بعض التشريعات التي تحتوي على قواعد تفصيلية للتفتيش تُطبق على مكوّنات الحاسب الآلي المادية في أحوال معينة، منها على سبيل المثال القسم 16-1 من قانون المنافسة الكندي؛ حيث يمنح الشخص الذي يحمل إذن بالتفتيش إمكانية استخدام أو العمل على استخدام أي نظام للحاسب الآلي للتفتيش على أي بيانات يحتويها أو تكون متاحة لهذا النظام أو يجوز له أن يسجل أو يعمل على تسجيل تلك البيانات في شكل مطبوعات أو أي مخرجات أخرى.

الفرع الثاني

تفتيش المكوّنات المنطقية لجهاز الكمبيوتر

تفتيش المكوّنات المنطقية – البرامج software – للحاسب الآلي أثار خلافاً كبيراً في الفقه بشأن جواز تفعيلها، ذهب رأي في الفقه إلى جواز

(1) الطواليه، علي حسن، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق.

ضبط البيانات الإليكترونية بمختلف أشكالها، ويستند هذا الرأي في ذلك إلى أن القوانين الإجرائية عندما تنص على إصدار الإذن بضبط «أي شيء»، فإن ذلك يجب تفسيره بحيث يشمل بيانات الكمبيوتر المحسوسة وغير المحسوسة، بينما ذهب رأي آخر إلى عدم انطباق المفهوم المادي على بيانات الحاسب غير المرئية أو غير الملموسة، ولذلك فإنه يقترح مواجهة هذا القصور التشريعي بالنص صراحة على أن تفتيش الكمبيوتر بحيث تُصبح الغاية الجديدة من التفتيش بعد التطور التقني الذي حدث بسبب ثورة الاتصالات عن بعد تتركّز في البحث عن الآجلة المادية أو أي مادة معالجة بواسطة الحاسب [1].

وفي مقابل هذين الرأيين يوجد رأي آخر نأى بنفسه عن البحث عما إذا كانت كلمة «شيء» تشمل البيانات المعنوية لمكوّنات الكمبيوتر أم لا، فذهب إلى أن النظرة في ذلك يجب أن تستند إلى الواقع العملي والذي يتطّلب أن يقع الضبط على بيانات الحاسب الآلي إذا اتخذت شكلاً مادياً.

ولذلك نجد أن القسم (94) من قانون الإجراءات الجنائية الألمانية ينص على أن: «الأدلة المضبوطة يجب أن تكون ملموسة»، وهي على هذا النحو تشمل ليس فقط نظم الكمبيوتر، بل أيضاً الدعامات التي تحمل عليها البيانات، ويترتّب على ذلك أن البيانات منفردة عن الدعامات لا تُعد أشياءً لكي يمكن ضبطها، ولكن إذا تم طبع هذه البيانات فإن مطبوعاتها تُعد من الأشياء الملموسة، وبالتالي يمكن ضبطها.

ويسير قانون العقوبات في رومانيا على ذات النهج، فطبقاً لهذا القانون فإن ضبط الأشياء بالنسبة للحاسب الآلي يشمل الجوانب المادية، والتي منها البيانات المحمّلة على الدعامات كالأشرطة المغناطيسية أو الأقراص، وأما البيانات ككيان معنوي فإنها لا تصلح للضبط، فإذا كانت البيانات ككيان

---

(1) رستم، هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، 1994م.

معنوي يصعب ضبطها، إلا أنها إذا حملت على دعامات أو تم تفريغها في شكل مستندات ،أو سجلات، فإنه يمكن ضبطها لأنها بذلك تكون قد تحولت إلى كيان مادي ملموس [1].

ويذهب رأي فقهي إلى أنه في تحديد مدلول الشيء بالنسبة لمكوّنات الكمبيوتر يجب عدم الخلط بين الحق الذهني للشخص على البرامج والكيانات المنطقية وبين طبيعة هذه البرامج والكائنات، وإنما يتعين الرجوع في ذلك إلى تحديد مدلول كلمة المادة في العلوم الطبيعية، فإذا كانت المادة تعرف بأنها كل ما يشغل حيزاً مادياً في فراغ معين وأن الحيز يمكن قياسه والتحكّم فيه، وكانت الكيانات المنطقية أو البرامج تشغل حيزاً مادياً في ذاكرة الكمبيوتر ويمكن قياسها بمقياس معين، وإنها أيضاً تأخذ شكل نبضات إليكترونية تُمثّل الرقمين صفر أو واحد، فإنها طبقاً لذلك ذات كيان مادي وتتشابه مع التيار الكهربائي الذي اعتبره الفقه والقضاء في فرنسا ومصر من قبيل الأشياء المادية. والمشكلة التي تُثيرها الجرائم التي تقع على الكيان المعنوي للكمبيوتر تتعلّق بإثبات الجرائم التي تقع عليها، فالضبط الذي قد يقع بسبب التفتيش لا يتصور وقوعه إلا إذا تبيَّن أن هناك جريمة قد ارتُكِبت [2].

ولذلك فإن الجرائم التي تُرتَكب على الكيانات المادية يسهل اكتشاف أمرها وضبطها، وأما الجرائم التي تُرتَكب على الكيانات المادية يسهل اكتشاف أمرها وضبطها، وأما الجرائم التي تقع على الكيانات المعنوية فإنه يصعب اكتشافها إذا ظلّت على صورتها المعنوية في شكل نبضات أو ذبذبات، وأما إذا تحوّلت هذه الكيانات إلى مستخرجات، أو مستندات، أو سجلات، فإنه يسهل الوصول إلى الجرائم التي تُرتَكب عليها.

---

(1) إبراهيم، خالد ممدوح الجرائم المعلوماتية، المرجع السابق.

(2) الصغير، جميل عبد الباقي، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، المرجع السابق.

ليس أدل على ذلك من أن سرقة التيار الكهربائي قد اعتبرها القضاء والفقه من قبيل الأشياء عندما وسع في مفهوم السرقة، بحيث يمكن أن تقع على الشيء أو منفعة الشيء، وهي على هذا النحو لا يمكن أن تتمخّض عنها جريمة السرقة إلا بوقوع الفعل المادي للسرقة المتمثّل في اختلاس التيار الكهربائي بتمريره خارج العداد الذي يحص كمية التيار الكهربائي المستهلكة، فلولا هذا السلوك المادي لما أمكن اكتشاف هذه الجريمة والعقاب عليها تحت وصف السرقة[1].

وبتطبيق ذلك على الجرائم التي تقع على الجوانب المعنوية للحاسبات الآلية فإنه لا يمكن العقاب عليها إلا بوقوع السلوك المادي الذي به تقوم الجريمة، فإذا وقعت جريمة سرقة أو تبديد أو تزوير أو غش على هذه الكيانات المعنوية، فإنه يصعب العقاب عليها إلا إذا ثبت التلاعب في هذه الكيانات المعنوية بشيء مادي ملموس يمكن الاستناد إليه للقول بتحقّق السلوك المادي الذي لا عقاب على أي جريمة إلا بتوافره، حتى ولو ثبت هذا التلاعب بعرض البيانات على شاشة الكمبيوتر وتم اكتشاف السلوك غير المشروع من خلال هذا العرض. فالبرنامج ككيان معنوي إذا تمثّل في مصنف مبتكر، فإنه يخضع للحماية الجنائية المقررة لحق المؤلّف، أما استعمال هذا البرنامج بواسطة الحاسبات الآلية كأداة في المجالات التي يستغل فيها البرنامج لارتكاب جرائم السرقة، أو نصب، أو تبديد، أو غش، أو تزوير، فإن هذه الجرائم لا تكون واقعة على حق المؤلّف الذي يحمي البرنامج ككيان ذهني مملوك لصاحبه، وإنما تكون واقعة على مجني عليهم آخرين هم الذين وقعت عليهم الأفعال التي يتحقّق بها السلوك المادي لهذه الجرائم [2].

---

(1) عرب، يونس، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، المرجع السابق.

(2) الطوالبه، علي حسن، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق.

الفرع الثالث

التفتيش عن بُعد

إن سلبية التكنولوجيا الرقمية قد عقدت من التحدي أمام أعمال التفتيش والضبط، فالبيانات التي تحتوي على أدلة قد تتوزّع عبر شبكة حاسبية في أماكن مجهولة بعيدة تماماً عن الموقع المادي للتفتيش، وإن ظل من الممكن الوصول إليها من خلال حواسيب تقع في الأبنية الجاري تفتيشها. وقد يكون الموقع الفعلي للبيانات داخل اختصاص قضائي آخر أو حتى في بلد آخر، في حين أن السلطات في بعض البلاد قد لا تنزعج من أن تقودها تحقيقاتها إليكترونياً إلى اختصاص قضائي سيادي آخر، إلا أن السلطات في ذلك الاختصاص السيادي قد تشعر ببالغ الانزعاج، وهذا يزيد من تعقيد مشاكل الجريمة المعلوماتية العابرة للحدود ويزيد من أهمية تبادل التعاون القضائي [1].

ونستطيع أن نُميز في هذه الصورة بين ثلاثة احتمالات على النحو التالي:

1 - اتصال حاسب المتهم بحاسب آخر أو نهاية طرفيه موجودة في مكان آخر داخل الدولة:

يُثار التساؤل حول مدى إمكانية امتداد الحق في التفتيش إذا تبيَّن أن الحاسب أو النهاية الطرفية في منزل المتهم متَّصلة بجهاز أو نهاية طرفيه في مكان آخر مملوك لشخص آخر خلاف المتهم.

ويرى الفقه الألماني إمكانية امتداد التفتيش إلى سجلات البيانات

---

(1) أحمد، هلالي عبد اللاه، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق.

التي تكون في موقع آخر استناداً إلى مقتضيات القسم (103) من قانون الإجراءات الجزائية الألماني.

ونجد إرهاصات هذا الرأي في المادة (88) من قانون تحقيق الجنايات البلجيكي التي تنص على: «إذا أمر قاضي التحقيق بالتفتيش في نظام معلوماتي، أو في جزء منه فإن هذا البحث يمكن أن يمتد إلى نظام معلوماتي آخر يوجد في مكان آخر غير مكان البحث الأصلي، ويتم هذا الامتداد وفقاً لضابطين [1]:

1 - إذا كان ضرورياً لكشف الحقيقة بشأن الجريمة محل البحث.

2 - إذا وجدت مخاطر تتعلّق بضياع بعض الأدلة نظراً لسهولة عملية محو، أو إتلاف، أو تحريف، أو نقل البيانات محل البحث.

ونجده في القانون الاتحادي الأسترالي حيث لم تعد صلاحيات التفتيش المتصلة بالأدلة الإليكترونية تقتصر على مواقع محدَّدة فقد توخّى قانون الجرائم المعلوماتية لعام 2001م إمكانية أن تتوزَّع بيانات الأدلة على شبكة حاسبات، ويسمح هذا القانون بعمليات تفتيش البيانات خارج المواقع التي يمكن اختراقها من خلال حواسيب توجد في الأبنية الجاري تفتيشها، ويُشير مصطلح البيانات المحتجزة في حاسوب ما إلى بيانات محتجزة في جهاز تخزين على شبكة حاسب يُشكِّل الحاسب جزء منها، فلا توجد حدود جغرافية محدَّدة، ولا أي اشتراط بالحصول على موافقة طرف ثالث.

غير أن المادة 3LB بقانون الجرائم لعام 1914م، والتي أدرجها قانون الجرائم المعلوماتية، تشترط إخطار شاغل المبنى النائي قدر الإمكان عملياً، وهذا قد يكون أكثر تعقيداً مما يبدو عليه، إذ أنه في مسار إجراء عملية بحث من خلال بيئة مرتبطة شبكياً، فإن المرء لا يكون متأكداً دائماً من مكان وجوده [2].

---

(1) عفيفي، عفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، 2003م.

(2) الطواليه، علي حسن، مشروعية الدليل الإليكتروني المستمد من التفتيش الجنائي، المرجع السابق.

2 - اتصال حاسب المتهم بحاسب آخر أو نهاية طرفيه موجودة في مكان آخر خارج الدولة:

من المشاكل التي تواجه سلطة الادعاء في جمع الأدلة والتحقيقات حالة امتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافي للدولة التي صدر من جهتها المختصة الإذن ودخوله في المجال الجغرافي لدولة أخرى، وهو ما يُسمَّى بالولوج أو التفتيش عبر الحدود قد يتعذَّر القيام به بسبب تمسُّك كل دولة بسيادتها.

لذا فإن جانب من الفقه يرى أن التفتيش الإليكتروني العابر للحدود لابد وأن يتم في إطار اتفاقيات تعاون خاصة ثنائية أو دولية تُجيز هذا الامتداد تعقد بين الدول المعنية، وبالتالي فإنه لا يجوز القيام بذلك التفتيش العابر للحدود في ظل غياب تلك الاتفاقية، أو على الأقل الحصول على إذن الدولة الأخرى، وهذا يؤكِّد على أهمية التعاون الدولي في مجال مكافحة الجرائم التي تقع في المجال الإليكتروني.

3 - التصنت والمراقبة الإليكترونية لشبكات الحاسب الآلي:

التصنُّت والأشكال الأخرى للمراقبة الإليكترونية رغم أنها مثيرة للجدل إلا أنه مسموح بها تحت ظروف معينة في جميع الدول تقريباً، فالقانون الفرنسي الصادر في 1991/7/10م يُجيز اعتراض الاتصالات البعيدة بما في ذلك شبكات تبادل المعلومات.

وفي هولندا أجاز المشرُّع القاضي التحقيق أن يأمر بالتصنُّت على شبكات الاتصالات إذا كانت هناك جرائم خطيرة ضالع فيها المتهم وتشمل هذه الشبكة التلكس والفاكس ونقل البيانات [1].

وفي اليابان أقر محكمة مقاطعة KOFU سنة 1991م شرعية التصنُّت على شبكات الكمبيوتر للبحث عن دليل.

---

(1) محمد، عادل ريان. (1995م)، جرائم الحاسب الآلي وأمن البيانات، العربي، (440)، 73 - 77.

المبحث الثاني

إجراءات تفتيش النظام المعلوماتي

تُعد إجراءات التفتيش والضبط من إجراءات التحقيق التي تختص بهما أصلاً سلطة التحقيق ولكن يُناط بمأموري الضبط القضائي من الأجهزة الأمنية القيام بهما في حالات استثنائية، ويُلاحظ أن التفتيش ليس غاية في ذاته، وإنما هو وسيلة للوصول من خلاله إلى أدلة في بيان وظهور الحقيقة وبذلك فإن التفتيش الباطل لا ينتج عنه إلا آثار باطلة وبالتالي يوجب عليه بطلان الأدلة الناتجة عن التفتيش والضبط.

ولا يكفي في التفتيش مجرد توافر شرطه سواء الموضوعية أم الشكلية، بل يلزم أيضاً ضرورة مراعاة حدوده الداخلية والتي يتمثّل أهمها في ضرورة التقيُّد بالغرض من التفتيش أثناء تنفيذه وفقاً لنص المادة (50) من قانون الإجراءات الجنائية والتي تقضي بأن الأصل في التفتيش هو البحث عن الأشياء المتعلّقة بالجريمة موضوع التحقيق[1].

المطلب الأوّل

إجراءات التفتيش الخاصة بالمتهم

محل ارتكاب الجريمة ينصب على نظام المعلومات الخاص بالمتهم دون تطلب التدخل في نظام معلوماتي لشخص آخر وفى هذا الفرض إذا كانت

(1) عفيفي، عفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، المرجع السابق.

الشروط الإجرائية للتفتيش صحيحة وفقا لتحديد أحكام محكمة النقض فإن التفتيش وما يسفر عنه من ضبط أي من الأدلة، سواء أكانت هذه الأدلة هي أجهزة الكمبيوتر، أم أحد الوسائط المتعددة يكون مشروعاً، وهذا الحال يكثر في جرائم التزوير والتزييف، حيث يتم التفتيش في أجهزة الكمبيوتر وملحقاته من طابعات ملوَّنة أو أجهزة ماسح ضوئي [1].

ويتم نقل البرنامج الداخلي الذي يوجد به عن طريق إتمام عملية التزوير أو التزييف في أي من الوسائط المتعدِّدة وبذلك يتم الحصول على دليل ارتكاب الجريمة، وهذا ما يتم أيضاً في جرائم النسخ والتقليد حيث يتم ضبط الوسائط المتعددة المحمَّلة بالبرامج المنسوخة والأجهزة المستخدمة في ذلك.

المطلب الثاني

إجراءات التفتيش التي لا تخص المتهم

هذا الفرض في مجال الجرائم التي تُرتَكب باستخدام الشبكات بحيث يتم ارتكاب الجريمة من أي أجهزة الحاسبات الآلية الأخرى والمتصلة بالحاسب الذي ارتُكب في نظامه المعلوماتي الجريمة وفي هذا الفرض فإن إجراءات التفتيش والضبط تتطلَّب الدخول في نظام معلوماتي لشخص آخر.

ويُلاحظ أنه طبقاً لنص المادة (45) من قانون الإجراءات الجنائية التي تنص على أنه: «لا يجوز لرجال السلطة العامة الدخول في أي محل مسكون إلا في الأحوال المبنية في القانون، أو في حالة طلب المساعدة من الداخل، أو

(1) أحمد، هلالي عبد اللاه، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق.

في حالة الحريق، أو الغرق، أو ما شابه»، بهدف حماية الخصوصية، وهو ما دعا المشرِّع إلى مد تلك الحماية إلى المحل الخاص بحيث أقر له ذات الحماية الخاصة بالمسكن، وكذلك السيارة الخاصة إذا كانت توجد في مسكن المتهم، أما إذا وجدت في الطريق العام فلها نفس حرمة الشخص بحيث لا يجوز تفتيشها إلا إذا جاز تفتيش الشخص قانوناً [1].

طبقاً لمعيار الخصوصية التي يحميها المشرِّع يتبيَّن أنه قد تناول المسكن والسيارة والمحل وكل ما يتعلَّق بالشخص وتتمثَّل خصوصياته؛ ولذلك فإن نظام المعلومات وما يحويه من خصوصيات للأشخاص تخضع أيضاً، وبالتبعية لمعيار الخصوصية من حيث عدم جواز التداخل فيه بدون إذن من النيابة العامة.

وهذا ما أكَّده المشرِّع عندما نص في قانون الأحوال المدنية المصري رقم (143) لسنة 1994 في المادة (13) فقرة (14) على أن: «تُعتبر البيانات والمعلومات المتعلِّقة بالأحوال المدنية للمواطنين، والتي تشمل عليها السجلات والدفاتر، أو الحاسبات الآلية، أو وسائط التخزين الملحَقة سرية ولا يجوز الاطلاع عليها، أو الحصول على بياناتها إلا في الأحوال التي نص عليها القانون ووفقاً لأحكامه»[2].

وهذا ما أكَّده الفقه أيضاً بامتداد الحق في التفتيش إلى سجلات البيانات التي تكون في موقع لآخر عندما يكون التخزين الفعلي خارج المكان الذي يتم فيه التفتيش.

وهذا ما أكَّده – جانب آخر من الفقه بأن البيانات لها طابع مادي على أساس أنها نبضات أو ذبذبات إليكترونية وإرشادات أو موجات كهرومغناطيسية

---

(1) حسين، محمد عبد الظاهر، المسئولية القانونية في مجال شبكات الانترنت، دار النهضة العربية، القاهرة 2002م.

(2) الطوالبه، علي حسن، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق.

قابلة لأن تسجل وتخزين على وسائط متعددة ويمكن قياسها. ونرى أنه فيما يتعلق بالعقبة تُمثلها طبيعة البيانات أو المعلومات من حيث كونها أشياء مادية لها القابلية في أن تكون محلاً لارتكاب الجرائم أم أن الأمر يختلف في هذا الصدد. ولأن البحث عن دليل على ارتكاب الجريمة، من حيث كونه وسيلة للإثبات ومحلاً لاقتناع وفقاً لنظرية الإثبات الجنائي يتطلّب الاتجاه السابق من آراء الفقهاء من حيث الإقرار بإمكانية أن تكون المعلومات محلاً لتفتيش وضبط الأدلة المتحصل عليها[1].

وهذا الأمر يختلف من حيث صدور إذن بالتفتيش في النظام المعلوماتي لأحد الأشخاص عنه في الإذن بالتفتيش في الجرائم التقليدية الأخرى؛ لأن الإذن قد يصدر في حق شخص قد ارتكب جناية أو جنحة وقامت قرائن قوية على ارتكابه للجريمة وعند القيام بتنفيذ إذن التفتيش، فإن الأمر قد يقتضي امتداد حق التفتيش إلى نظام معلوماتي آخر إما تابع للمتهم، أو أن للمتهم أكثر من جهاز في أماكن مختلفة، كأن يكون المتهم مالكاً في منزله وجهاز آخر في عمله، أو أن يكون الشخص له شريك في الأجهزة مما يتطلب الحصول على إذن آخر من النيابة العامة [2].

ويجب أن يتصف إذن الصادر من النيابة العامة بالمرونة من حيث إتاحة مساحة واسعة لمأموري الضبط في تنفيذ الإذن بالتفتيش ولكن بضوابط معنية بحيث يؤدي ذلك إلى البعد عن الهدف المقصود من صدور الإذن. وذلك عن طريق تحديد مجال هذا التفتيش وما يستتبعه بالضرورة من تتبع خلال شبكات المعلومات، ويخضع تقدير ذلك لسلطة القاضي التقديرية من حيث توافر حالة الضرورة أو عدم توافرها وهذا النظام اتبعته بعض الدول مثل الولايات المتحدة الأمريكية وكندا، حيث نصتا على أن يكون إذن التفتيش

---

(1) علي، عبد الصبور عبد القوي، الجريمة الإليكترونية، دار العلوم للنشر والتوزيع، القاهرة 2007م.

(2) رستم، هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، المرجع السابق.

متضمناً الآتي [1]:

1 - البحث عن أدلة محصلة من كيان الحاسب المنطقي والتي يدخل فيها برامج التطبيق ونظم التشغيل.

2 - البيانات المستخدَمة بواسطة برنامج الحاسب أو كيانه المنطقي.

3 - السجلات التي تثبت استخدام الأنظمة الآلية لمعالجة البيانات.

4 - السجلات المستخدمة في عملية الولوج في النظام الآلي لمعالجة البيانات، وبالتالي يتضح إلى أي مدى يتصف إذن النيابة بالمرونة حيث يمكن مأموري الضبط القضائي من مباشرة أعمالهم.

5 - الضمانات التي يجب أن تخول للأشخاص ما يلي:

- عدم اعتبار النظام المعلوماتي للشخص وبما له من خصوصية يخضع لذات الحماية المقررة لحرمة المسكن والسيارة الخاصة والمراسلات.

- عدم التعرُّض له إلا وفقاً للضوابط التي قررها المشرِّع لمأموري الضبط القضائي في مباشرتهم للإجراءات السابقة.

6 - التعاون الدولي في مواجهة امتداد إجراءات التفتيش والضبط خارج حدود الدولة.

تضطلع الجهات الأمنية بوزارة الداخلية بمواجهة الجريمة بشتى صورها وفى جميع مراحلها أي قبل وقوعها وهو محور وظيفتها من حيث من حيث كونها ضبطية إدارية أو تعقب الجريمة بعد وقوعها أي ضبط مرتكبيها وضبط ما يسفر عنه من أدلة، وهو أساس وظيفتها كضبطية قضائية. وتُباشر

(1) الطواليه، علي حسن، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق.

في ضوء ذلك الأجهزة الأمنية وظيفتها في ضوء، ونتيجة لكون الإجرام المعلوماتي ظاهرة مستخدَمة على الساحة الإجرامية داخلي جمهورية مصر العربية لم ينص قانون العقوبات بالنص عليها صراحة أو ما يمكن تطبيقه من النصوص القانونية المطبقة في الجرائم التقليدية. وتبين كذلك أن تعقب مرتكب الجريمة وتتبع آثاره وضبط الأدلة المعلوماتية الدالة على ارتكابه لجريمة قد لا يتقيد بحدود القطر وإنما يمتد إلى خارجه، وهذا مرجعه إلى ظهور شبكات الكمبيوتر التي ربطت جميع الدول ببعضها البعض وأصبح لا يحدها فاصل، وأمام هذا التطور التكنولوجي بات ارتكاب الجرائم من دولة إلى أخرى من السهولة بمكان ولذلك أصبح من ضروري البحث في مشروعية القيام بإجراء التفتيش والضبط من قبل مأموري الضبط القضائي لمتهم في دولة أخرى [1].

وتعرف الجريمة بهذا الوصف بالجريمة المنظمة نتيجة مزاولة الأنشطة الإجرامية عبر حدود الدول، ما دعا الدول لإقرار أن الجريمة المنظمة هي في حقيقتها جريمة داخلية مضافاً إليها البعد الدولي، أي بارتكابها خارج حدود القطر وحدوث النتيجة داخله.

وإذا كان الاختصاص بنظر تلك الجرائم ينعقد للاختصاص المكاني للدولة التي حدث ارتكاب الجريمة على أرضها تبعاً لمبدأ سيادة الدولة، فإن لمأموري الضبط القضائي القيام بإجراءات التفتيش والضبط على أراضيها.

وهنا يثور البحث في حالة امتداد إجراءات التفتيش والضبط خارج حدود الدولة والدخول في سيادة دولة أخرى. لذلك فإن الدول حرصاً منها على مراعاة مصلحتين هامتين هما احترام الخصوصية للأشخاص ومواجهة الجرائم المرتَكبة لتحقيق الصالح العام أبرمت العديد من الاتفاقيات الدولية لمكافحة هذه الظاهرة، هذا بجانب الضمانات التي أقرَّتها المواثيق الدولية [2].

---

(1) عفيفي، عفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، المرجع السابق.

(2) علي، عبد الصبور عبد القوي، الجريمة الإليكترونية، المرجع السابق.

المبحث الثالث

شروط الإذن الصادر بتفتيش الوسائل المعلوماتية

لكي يكون الإذن بالتفتيش صحيحاً يجب أن يكون مَن أصدر الإذن مختصاً بالتحقيق في الجريمة التي يصدر الإذن بشأنها، وهذا الاختصاص قد يتحدد بمحل الواقعة أو المكان الذي ضبط فيه الجاني أو بمحل إقامته. ويجوز أن تمتد بعض الإجراءات خارج هذا الاختصاص إذا استوجبت ظروف التحقيق ذلك بشرط أن يكون المحقّق قد بدأ إجراءات التحقيق بدائرة اختصاصه المكاني. ويلزم كذلك أن يكون المحقّق مختصاً بالإجراء الذي يتخذه، فلا يجوز له ندب مأمور الضبط القضائي لتفتيش غير المتهم أو غير منزله لأن هذا التفتيش يخرج عن اختصاصه. ويجب لصحة إذن التفتيش الصادر في محيط الجرائم التي تقع على الوسائل المعلوماتية أو عن طريقها أن يكون مَن صدر له الإذن بالتفتيش من مأموري الضبط القضائي المختصين بذلك وظيفياً ومكانياً ونوعياً، ولا يشترط بعد ذلك التزام المحقق بندب مأمور ضبط معين. وإذا كانت الجرائم التي تقع بالوسائل الإليكترونية أو عليها ذات طبيعة فنية فإنه ينبغي توافر خبرة معينة في مأمور الإذن القضائي الذي يندب لتفتيش نظم الوسائل المعلوماتية لكي يتمكن من تأدية عمله وفي ذات الوقت يحافظ على سلامة الأدلة المتحصلة من الجريمة المعلوماتية، ويشترط في الإذن بالتفتيش الصادر بالنسبة للجرائم التي تقع في محيط الوسائل الإليكترونية أن يكون مكتوباً ومحدداً التاريخ وموقعاً ممَّن أصدره، وأن يكون صريحاً في الدلالة على التفويض في مباشرة التفتيش، وأن يتضمن من البيانات ما يُحدد نوع الجريمة المطلوب جمع الأدلة عنها. ويجب كذلك تحديد محل التفتيش والذي قد يكون شخصاً أو منزلاً، وتحديد المدة الزمنية التي يراها المحقق كافية لتنفيذ الإذن. ولا شك في أن تحديد محل التفتيش تحديداً دقيقاً بالنسبة للجرائم المعلوماتية قد تكتنفه بعض الصعوبة، ذلك

أن تحديد كل أو بعض مكوّنات الوسائل المعلوماتية وإيرادها في إذن التفتيش وتحديدها تحديداً دقيقاً قد يستلزم ثقافة فنية عالية في تقنية الحاسب الآلي، فلا لا تتوافر للمحقق أو لمأمور الضبط القضائي. وإذا كانت الجرائم التي تقع في محيط الوسائل المعلوماتية تتميز بطبيعة فنية متأثرة في ذلك بالطبيعة الفنية للعمليات الإليكترونية [1].

(1) رستم، هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، المرجع السابق.

المبحث الرابع

مشكلات التفتيش في الجرائم المعلوماتية

وفيما يخص محل التفتيش وما في حكمه في البيئة المعلوماتية، فهو قد يرد على المكوّنات المادية للحاسب الآلي وملحقاته، وهذه لا خلاف يُذكر حول خضوعها للتفتيش والضبط طبقاً لقواعد قانون الإجراءات الجنائية، بما في ذلك البيانات المخزّنة في أوعية أو وسائل مادية كالأشرطة الممغنطة والأقراص الصلبة والضوئية، وذلك تبعاً للمكان أو الحيّز الموجودة فيه[1]. ومن ثم، إذا كانت موجودة بمسكن المتهم أو أحد ملحقاته فتحكمها القواعد ذاتها التي يخضع لها تفتيش المسكن؛ إذ يجوز تفتيشها وضبطها متى كان تفتيش المسكن جائزاً، والعكس صحيح. وفي حال وجودها في مكان عام فيحكمها ما يحكم هذا المكان من أحكام، وهلم جراً، في حين أنه إذا كان الحاسب في حوزة شخص خارج مسكنه، فإن تفتيشه عندئذٍ يخضع للقواعد ذاتها التي يخضع لها تفتيش الشخص بوصفه أحد متعلقاته، يستوي أن يكون الحائز هو مالك الجهاز أم سواه.

ومن ناحية أخرى، وهو الأهم الذي يعنينا بالذات، أن التفتيش وما في حكمه قد يرد على الجانب المنطقي للحاسوب، المتمثّل في المعلومات والبيانات المعالجة إليكترونياً، وهي محل جدل كبير حول صلاحيتها لأن تكون موضوعاً للتفتيش والضبط من عدمها[2]. فثمة اتجاه يرى أن هذه المكوّنات المنطقية لا تصلح بطبيعتها لأن تكون كذلك، على اعتبار أن التفتيش يهدف في المقام الأول إلى ضبط أدلة مادية، وهذا يستلزم وجود أحكام خاصة تكون أكثر ملائمة لهذه البيانات غير المحسوسة.

---

(1) إبراهيم، خالد ممدوح الجرائم المعلوماتية، المرجع السابق.

(2) أحمد، هلالي عبدا للاه، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق.

وثمة اتجاه آخر يقول بأن المكوّنات المعنوية لا تختلف عن الكيان المادي للحاسب الآلي من حيث خضوعها لأحكام التفتيش وما في حكمه، بدعوى أن البيانات، التي هي عبارة عن نبضات إليكترونية، قابلة للتخزين على أوعية أو وسائط مادية كالأشرطة الممغنطة والأقراص والأسطوانات، كذلك يمكن تقديرها وقياسها بوحدات قياس خاصة معروفة، وعلى هذا الأساس تكون صالحة كموضوع للضبط والتفتيش شأنها شأن الوسائط المادية ذاتها.

واتجه بعض الفقهاء إلى أن الاتجاه الأول أكثر منطقية؛ ذلك أن القواعد التي تحكم التفتيش والضبط إنما وُضعت في زمن مبكر وقبل ظهور الحاسب وتطبيقاته، وأياً كانت المبررات التي ساقها معتنقو المساواة بين الكيان المادي والمنطقي، فإن طبيعة البيانات المعالجة تتطلّب قواعد خاصة تحكمها بدلاً من محاولة تطويع القواعد التقليدية وتوسيع نطاقها، وهذا يتأتّى من خلال إجراء تعديل عليها من شأنه توسيع نطاق الأشياء التي تكون مشمولة بالتفتيش والضبط وتضمينها من الأحكام بما يتلاءم ومتطلبات هذه التقنية الجديدة. فالنصوص الخاصة بالتفتيش بمعناه التقليدي لا ينبغي إعمالها بشأنها مباشرة، باعتبار أن هذه النصوص تُمثل قيداً على الحرية الفردية، ومن ثَم يصبح القياس على الأشياء المادية محظوراً لمنافاته الشرعية الإجرائية [1].

وباستقراء موقف التشريعات الحديثة نجدها قد ذهبت إلى تأكيد هذا الاتجاه، بحيث أضحت المكوّنات المعنوية للحاسب الآلي ضمن الأشياء التي تصلح أن تكون محلاً للتفتيش والضبط. ففي التشريع الأمريكي على سبيل المثال تقضي المادة (34) من القواعد الفيدرالية الخاصة بالإجراءات الجنائية الصادرة سنة 1970م بعد تعديلها بمد نطاق التفتيش ليشمل ضمن ما يشمل أجهزة الحاسب الآلي وأوعية التخزين والبريد الإليكتروني والصوتي والمنقول

(1) رستم، هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، المرجع السابق.

عن طريق الفاكس. فضلاً عن آن الاتفاقية الأوروبية للجريمة الافتراضية (اتفاقية بودابست) تقضي في المادة (19) منها بإلزام الدول الأطراف في هذه الاتفاقية بضرورة تبني التدابير والإجراءات التشريعية التي تخول السلطات المختصة ولوج البيئة المعلوماتية، وذلك من أجل تيسير إثبات هذه الجرائم. ومع هذا، نلاحظ أن بعض أحكام القضاء المقارن قد تبنّت التفسير الموسّع لمدلول الأشياء محل الضبط والتفتيش، بحيث ينسحب على بيانات الحاسب الآلي حتى في غياب نصوص خاصة تحكم هذه المسألة. وهو اتجاه نرى أنه محل نظر، ولكن، ماذا لو كان النظام المعلوماتي مزوداً بنظام حماية يمنع من ولوجه دون تدخل القائم على هذه المنظومة ومساعدته ؟ فهل يا ترى يجوز إجبار المتهم مثلاً على تزويد السلطات المختصة بالتحقيق بمفاتيح المرور إلى النظام المعلوماتي؟ أو بالأحرى هل يمكن إكراهه على الإفصاح عن كلمة السر وما في حكمها من أجل تسهيل الولوج إلى البيئة المعلوماتية؟ (1)

وثمة رأي يرفض إجبار المتهم على تقديم المعلومات اللازمة لتسهيل ولوج النظام المعلوماتي. والحجة التي يستند إليها هذا الرأي تتجسد في قاعدة معروفة ومستقرة أن المتهم لا يجوز إجباره على الإجابة عن الأسئلة التي من شأنها أن تفضي إلى إدانته؛ إذ من حقه الاعتصام بالصمت دون أن يُفسَّر ذلك الصمت ضد مصلحته. وهذا الاتجاه اعتنقته بعض التشريعات الحديثة، ومنها القانون الياباني الذي يحظر على الأجهزة المختصة إكراه مالك الحاسب الآلي على الإفصاح عن كلمة المرور أو السر Password، والنهج ذاته كان قد تبناه مشروع قانون الإجراءات الجنائية البولندي. وفي المقابل، ذهب رأي آخر إلى القول بأنه« وإن كان لا يجوز إجبار الشخص على الإدلاء بأقواله ضد نفسه، بيد أن ذلك لا ينبغي أن يكون حائلاً دون إجباره

---

(1) الطوالبه، علي حسن، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، المرجع السابق.

على تقديم معلومات يقتضيها ولوج النظام المعلوماتي للسلطات المختصة، متى كانت هذه المعلومات بحوزته، قياساً على إجبار الشخص على تسليم مفتاح الخزنة الذي بحوزته» [1].

ولكن هذا الرأي الأخير أياً كانت المبررات التي يقوم عليها، لا يمكن القبول به، فقياس المعلومة التي بحوزة المتهم على مفتاح الخزنة وما في حكمه قياس مع الفارق. ذلك أن المعلومة (المتمثلة في كلمة السّر وما في حكمها) هي أمر معنوي بخلاف المفتاح الذي هو شيء مادي محسوس قابل للتسليم. هذا من ناحية، ومن ناحية أخرى فإن هذا الرأي الأخير لا يتفق مع الأصول المستقرة في الإثبات الجنائي، ويتنافى مع مقتضيات حق الدفاع أمام القضاء الجنائي. ومن ناحية ثالثة، وحتى على فرض التسليم بجواز إكراه المتهم أو المشتَبه به على تقديم مفاتيح الشفرة التي تمكّن من ولوج النظام المعلوماتي، فإن الأمر تكتنفه صعوبات عملية لا يمكن التغلب عليها، لعل أبرزها أن المتهم يستطيع التذرُّع بنسيان المعلومة أو عدم إمكان تذكرها أو ما شابه ذلك. وهذا يعني ببساطة أن الرأي الأول أدعى إلى القبول، ولكن ليس على إطلاقه؛ إذ يجوز إجبار غير المتهم على تقديم المعلومة التي من شأنها تيسير الدخول إلى المنظومة كمقدم الخدمة مثلاً، وذلك بحمله على الإفصاح عن كلمة السر التي بحوزته للوصول إلى المصدر أو شبكة الاتصالات؛ لأن الإكراه الواقع على غير المتهم لا يمس حقوق الدفاع خلافاً للوضع بالنسبة للمتهم [2].

وقد يكون حاسب المتهم متصلاً بغيره من الحواسيب عبر شبكة، وهنا ينبغي التمييز بين ما إذا كان حاسوب المتهم متصلاً بآخر داخل إقليم الدولة أو كان متصلاً بحاسوب يقع في نطاق إقليم دولة أخرى [3]:

---

(1) علي، عبد الصبور عبد القوي، الجريمة الالكترونية، المرجع السابق.

(2) عرب، يونس، قانون الكمبيوتر، موسوعة القانون وتقنية المعلومات، المرجع السابق.

(3) قشقوش، هدى، جرائم الحاسب الإليكتروني في التشريع المقارن، الطبعة الأولى، دار النهضة العربية، القاهرة، 1992م.

المطلب الأوّل

حالة اتصال حاسب المتهم بحاسب آخر داخل الدولة

لو نظرنا إلى القواعد العامة للتفتيش في معظم الدول والتي تقضي بأنه لا يجوز إجراؤه من النيابة العامة إلّا بعد الحصول على إذن من القاضي الجزئي. هذا إذا كان التحقيق يُباشر من قِبلها، أما إذا كان الذي يباشره قاضي التحقيق نفسه، فلا يستلزم حصول هذا الإذن. وبناءً على ذلك، فإذا كان الحاسوب موجوداً بمنزل غير المتهم فلا يجوز تفتيشه من قِبل النيابة العامة إلّا بعد استصدار إذن من القاضي الجزئي قبل ولوجه، وإلّا كان الإجراء باطلاً وغير مثمر. غير أن صدور الإذن قد يستغرق بعض الوقت، ما قد يؤدي إلى تلاشي الدليل واندثاره بالمحو والإتلاف، وهذا ربما يُعيق الوصول إلى الدليل وتحصيله [1].

و كما تقدم فالجاني قد يحاول العبث بالدليل كي لا ينكشف أمره قبل صدور الإذن، لاسيما وأنه يستلزم تحديد محل الإذن بدقة حتى يتسنى تنفيذه، وهذا دون شك ينطوي على شيء من العنت والصعوبة سواء بالنسبة للنادب (مصدر الإذن) أو الجهة المنفّذة للإذن، سيما إذا آخذنا في الاعتبار أن هذه الأجهزة تفتقر إلى الخبرة اللازمة في هذا المجال الفني. ولهذا رُئي بحق ضرورة معالجة هذه المشكلة بنص خاص يقضي بتوسيع سلطات الجهة المعنية بإجراء التفتيش، ولو استلزم الأمر ولوج النظام المعلوماتي دون الحصول على إذن عند الضرورة، إذا كان من شأن انتظار صدور الإذن أن يفوت فرصة الحصول على الدليل. وقد تبنّت بعض التشريعات المقارنة هذا الاتجاه، ومنها قانون تحقيق الجنايات البلجيكي الصادر في 23 نوفمبر 2000م م الذي

(1) الطويل، خالد بن محمد، التعامل مع الاعتداءات الإليكترونية من الناحية الأمنية مركز المعلومات الوطني، وزارة الداخلية، المرجع السابق.

يُجيز امتداد التفتيش إلى نظام معلوماتي آخر غير مكان البحث الأصلي، ولكن ليس بصورة مطلقة وإنما بقيود معينة، يمكن إجمالها في أن تكون ثمة ضرورة لكشف الحقيقة فيما يخص الجريمة موضوع البحث أو أن تكون الأدلة معرَّضة لمخاطر معينة كالإتلاف أو التدمير وما شابه.

وقد تقر الاتفاقية الأوروبية للجرائم المعلوماتية ذلك متى كانت المعلومات المخزَّنة بحاسب غير المتهم يتم الدخول إليها من خلال الحاسب الأصلي محل التفتيش [1].

وفي الولايات المتحدة الأمريكية تجيز المادة (a 41) من قانون الإجراءات الجنائية الفيدرالي الأمريكي لقاضي التحقيق إصدار إذن تفتيش ملكية داخل منطقة أو خارجها، متى كانت الملكية عند طلب الإذن موجودة داخل المنطقة، ولكن يخشى أو يتوقع تحركها خارج المنطقة قبل تنفيذ الإذن، وربما المشكلة التي تواجه رجال الضبط عند تنفيذهم التفتيش أنه لا يكون باستطاعتهم التحقّق من أن البيانات المضبوطة جرى تخزينها داخل المنطقة أم خارجها.

المطلب الثاني

حالة اتصال حاسب المتهم بحاسب آخر في دولة أخرى

تعددت الاتجاهات حول مدى امتداد التفتيش للحاسبات الأخرى خارج الدولة، (فذهب رأي إلى رفض امتداد التفتيش للحاسبات المتصلة بحاسب المتهم خارج الدولة، بدعوى أن ذلك ينطوي على انتهاك لسيادة دولة أخرى، أو بالأحرى يُشكّل اعتداءً على ولاية الدولة التي يجري التفتيش في نطاق

(1) عفيفي، عفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، المرجع السابق.

إقليمها، ومن ثَم فالأمر يتطلب لجوء سلطات التحقيق إلى سلوك الإجراءات المعتادة بطلب المساعدة القضائية، أو الإنابة القضائية من السلطات الموازية في الدولة الأخرى [1].

وإن مباشرة هذا الإجراء تستلزم وجود اتفاقية وإلّا يفقد مشروعيته. ولأجل مواجهة هذه المشكلة في نظر الفقه المقارن ينبغي التماس طلب من سلطات الدولة الأخرى بنسخ البيانات المخزَّنة في الحاسبات الموجودة على أراضيها وإرسالها إلى الدولة الطالبة. غير أن هذا الأسلوب المعروف بأسلوب التفويض والالتماس يُعاب عليه أنه يفتقر إلى الفعالية دولية، لإجراءات الروتينية التي تفضي إلى تأخير الوصول إلى الدليل وربما ضياعه أو إتلافه. والاتجاه الرافض لامتداد التفتيش إلى الحاسبات الأخرى لا يقر هذا الإجراء إلّا بموجب اتفاقية دولية، وهو يعبر عن الرأي السائد في الفقه الألماني [2].

وسيراً في هذا الاتجاه، عرضت على القضاء الألماني واقعة تتعلّق بالغش المعلوماتي، الفرنسي. طرفية الحاسب الموجودة بألمانيا متصلة بأخرى بسويسرا. وبالرغم من أن السلطات الألمانية قد حاولت استرجاع البيانات المخزَّنة بالخارج، إلّا أنها لم تتمكن من ذلك إلّا من خلال التماس المساعدة المتبادلة وأدل على ذلك سلطة التحقيق.

وثمة جانب آخر من الفقه أمر امتداد التفتيش إلى الحاسبات الموجودة خارج إقليم الدولة، وهذا الرأي يقوم على أساس واقعي؛ إذ إن معتنقيه والمدافعين عنه يحاولون التعامل بواقعية مع ما يعترض سلطات التحقيق من مشكلات. وهذا الاتجاه أخذ به القانون الفرنسي من خلال المادة (17) من قانون الأمن الداخلي الفرنسي. كما يسمح قانون التحقيق البلجيكي (مادة 88) لقاضي التحقيق الحصول على نسخة من البيانات التي هو في حاجة إليها دونما انتظار إذن من سلطات الدولة الأخرى، ويُحاول الفقه الفرنسي

(1) عرب، يونس، قانون الكمبيوتر، موسوعة القانون وتقنية المعلومات، المرجع السابق.

(2) قشقوش، هدى، جرائم الحاسب الإليكتروني في التشريع المقارن، المرجع السابق.

تبرير هذا الاتجاه بأن العالم الافتراضي لا يعرف الحدود، ومع هذا فالفقه هناك يسلّم بأن النص المذكور يُمثل انتهاكاً لسيادة الدول الأخرى. كذلك تُجيز المادة (32) من الاتفاقية الأوروبية للجرائم الافتراضية ولوج شبكة المعلومات التابعة لدولة أخرى لأجل التفتيش والضبط متى كان هذا الإجراء يتعلق بمعلومات، أو بيانات مباحة للجمهور، وأيضاً في حالة الحصول على رضا صاحب أو حائز هذه البيانات بالتفتيش[1].

والأمر في الولايات المتحدة الأمريكية يتوقف على وضع الشخص الذي ينفذ التفتيش، فإذا كان قبل مباشرته يعلم بأن البيانات والمعلومات المراد بحثها مخزّنة بعيداً في نطاق دولة أخرى، فعندئذٍ يستلزم التماس طلب مساعدة يتم توجيهه إلى سلطات الدولة الأخرى، أما إذا كان القائم بالتفتيش يجهل أو ليس في وسعه معرفة أن البيانات المراد تفتيشها خارج المنطقة، فإن ما يُسفر عنه التفتيش من ضبط لا يهدر، ويمكن قبوله والركون إليه في الإثبات بوصفه دليلاً مشروعاً متى ما اطمأنّت إليه المحكمة. والجدير بالذكر في هذا المقام أن المحاكم الأمريكية درجت على رفض دعاوى بطلان الدليل في حالة عدم استطاعة رجال الضبط معرفة ما إذا كان تنفيذ التفتيش يُشكّل إنتهاكاً للمادة (41) قانوناً أو فعلياً ما لم يتعمّد هؤلاء عدم إعمال القاعدة المذكورة، أو أن يكون لديهم حدس مُسبق [2].

ومن جهة أخرى فتنفيذ إذن التفتيش يُثير بعض الصعوبات في مجال الجرائم المعلوماتية في القانون سالف الذكر، ففي هذا القانون ثمة مبدأ يجب أن يلتزم به رجال الضبط القضائي، ألا وهو ضرورة الإعلان عن وجودهم والإفصاح عن السلطات المخولة لهم. بيد أن هذه القاعدة العامة يمكن التحلل

---

(1) Criminal Profiling: An Introduction to Behavioral Evidence Analysis,by Brent E. Turvey, Diana Tamlyn, Jerry Chisum, 1 edition, Academic Press Limited 1999.م

(2) الطوالبه، علي حسن، التفتيش الجنائي على نظم الحاسوب والانترنت – دراسة مقارنة، المرجع السابق.

منها وعدم الالتزام بها على كما ورد في أحد أحكام المحكمة الفيدرالية الأمريكية العليا متى كان مأمور الضبط القضائي قد توافر لديه شك مبرر في أن إعمال هذه القاعدة أو التقيُّد بها سيكون غير مجدٍ أو من شأنه إعاقة فعالية التحقيق، أو من المتوقع أن تنجم عنه خطورة ما [1].

المطلب الثالث

ضبط المراسلات عبر الانترنت

وفقاً لما هو وارد في قانون الإجراءات الجزئية في إحدى الدول[2] يجوز للنيابة مراقبة المكالمات الهاتفية والرسائل البريدية والبرقيات وما في حكمها بعد الحصول على إذن من القاضي الجزئي. ولا يجوز مباشرته بدون إذن نظراً لخطورة الإجراء المذكور باعتباره يمس حرمة الحياة الخاصة. وهذا النص لم يشمل صراحةً مراقبة وضبط الاتصالات الإليكترونية بجميع صورها وأشكالها بما في ذلك الرسائل الإليكترونية، ومع ذلك يمكن اعتبار هذا الأمر جائزاً ومشمولاً بالنص المشار إليه بصورة ضمنية، حيث يتسع مفهوم الرسائل إلى أبعد من المفهوم التقليدي لها، والإجراء ذاته مسموح به في الدول الأخرى بما فيها الولايات المتحدة الأمريكية وفرنسا وكندا واليابان وهولندا، ففي الولايات المتحدة الأمريكية مثلاً يُجيز القانون اعتراض الاتصالات الإليكترونية بصفة عامة بما في ذلك شبكات الحاسب الآلي، وذلك متى تم بإذن من المحكمة.

كما أن القانون الفرنسي الصادر في 10 يوليو سنة 1991م يسمح هو الآخر باعتراض الاتصالات البعيدة ومنها شبكة المعلومات، فضلاً عن

(1) قشقوش، هدى، جرائم الحاسب الإليكتروني في التشريع المقارن، المرجع السابق.

(2) المادة (180) من قانون الإجراءات الجنائية الليبي.

أن القانون الهولندي يُجيز إجراء التصنُّت على شبكة الحاسب الآلي بموجب أمر أو إذن من قاضي التحقيق، متى ثبت أن المتهم كان ضالعاً في جرائم خطيرة، ويشمل ذلك كل وسائل الاتصال بما في ذلك التلكس Telex، والفاكس Telefax ونقل البيانات.

المطلب الرابع

ضوابط التفتيش الوسائل المعلوماتية

التفتيش إجراء من إجراءات التحقيق تصدره سلطة تحقيق مختصة بهدف جمع الأدلة عن جريمة تُشكل جناية أو جنحة تكون قد وقعت بالفعل. وهو بالنسبة للوسائل الإليكترونية يتخذ ذات هذا التعريف ولكن محله يكون بالنسبة للجرائم التي تقع على الوسائل الإليكترونية بكياناتها المادية والمعنوية أو الجرائم التي تقع بواسطتها. وإذا كان هذا التفتيش لضبط أدلة جريمة تكون قد وقعت وأنه يمس حرية الأشخاص وحرمة مساكنهم.

لا محل للتفتيش بالنسبة للجرائم التي تقع على الوسائل الإليكترونية أو التي تقع بها، إلا إذا كانت هناك جريمة قد وقعت على هذه الوسائل، أو من هذه الوسائل، وأن تكون هذه الجريمة جناية أو جنحة، ومن أمثلة هذه الجرائم، الغش المرتبط بالحاسب الآلي: ويشمل الإدخال، الإتلاف، المحو، أو الطمس لبيانات أو برامج الحاسب الآلي، التزوير المعلوماتي: يتضمن الإدخال، الإتلاف، المحو أو الطمس البيانات أو برامج الحاسب، الإضرار ببيانات وبرنامج الحاسبات: ويشمل المحو، الإتلاف، التعطيل أو الطمس غير المشروع لبيانات وبرامج المعلوماتية، تخريب الحاسبات: ويحتوي على الإدخال، الإتلاف، المحو، أو الطمس لبيانات وبرامج الحاسب، الدخول غير المصرح به: وهو الدخول غير المشروع لنظام معلوماتي أو مجموعة نظم، وأخيراً:

الاعتراض غير المصرح به: وهو اعتراض غير مصرح به ويتم بدون وجه حق عن طريق استخدام وسائل فنية للاتصال. فلكي يصدر الإذن بتفتيش الوسائل الإليكترونية لجمع الأدلة عن جرائم تعد هذه الوسائل محلاً لها، فإن هذا التفتيش لا يكون صحيحاً إلا إذا كانت الجريمة التي يراد جمع الأدلة عنها ذات جسامة معينة بأن تكون من قبيل الجنايات أو الجنح، فيستبعد من نطاقها المخالفات، ولا يشترط أن تكون الجنحة معاقَب عليها بالحبس في حدود معينة، وإنما يكفي أن تكون الواقعة محل التفتيش تتمخَّض عنها جريمة من نوع الجنح. ويُلاحظ أنه لا محل لإصدار الإذن بتفتيش الحاسبات الآلية إلا إذا كان المشرِّع قد نص على الجرائم التي تُشكِّل اعتداء عليها في شكل نصوص التجريم والعقاب تطبيقاً لمبدأ شرعية الجرائم والعقوبات، وعلى النحو الذي فعلته الكثير من التشريعات المقارنة، وفعله المشرِّع المصري بالنسبة لبرامج الحاسب الآلي وقواعد البيانات سواء كانت مقروءة من الحاسب الآلي أو من غيره، إذ أنزل عليها حماية جنائية وجعل الاعتداء عليها يُعد جريمة من نوع الجنح على النحو الذي نصت عليه المادتين 140 و181 من القانون رقم 82 لسنة 2002 م بشأن حماية حقوق الملكية الفكرية [1].

أنزل المشرِّع المصري حمايته الجنائية على البرامج وقواعد البيانات المتعلِّقة بالأحوال المدنية للمواطنين، والبيانات الفردية التي تقتضي إجراء إحصاء للسكان وعلى النحو سالف الإشارة إليه. ولا يكفي لإصدار الإذن بتفتيش الوسائل الإليكترونية مجرد الإبلاغ بوقوع جريمة من قبيل الجناية أو الجنحة وإنما التي قد تصلح أن تكون قد تجمعت بالنسبة لها إمارات قوية تفيد وقوعها بما يُبرر المساس بحرية الأفراد عند تفتيش أشخاصهم، أو بحرمة منازلهم عند تفتيش هذه المنازل، والمعيار لإصدار الإذن بالتفتيش أن تكون الدلائل التي تجمعت حول الجريمة تدعو للاعتقاد المعقول بوقوعها سواء أكان من تجمعت حوله هذه الدلائل فاعلاً أصلياً لها أم يقف دوره

---

(1) أحمد، هلالي عبداللاه، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق.

الإجرامي عند الشريك. وتقدير هذه الدلائل متروك للسلطة التي تصدر الإذن بالتفتيش بشرط أن يكون تقديرها منطقياً ومتفقاً مع الواقع بحيث تكشف هذه الدلائل بجدية عن وقوع الجريمة محل الإذن بالتفتيش وأن هناك جانبا تنسب إليه. فالمنطق المجرد غير المعقول لا يكفي لإلقاء المصداقية على الدلائل التي تبرر المساس بحريات الأشخاص، وإنما لضبطها، يكون تقدير هذه الإمارات متّصفاً بالتعقل ومتفقاً مع ما درجت عليه قواعد الخبرة. وبناء على ذلك فإن الإذن بالتفتيش لا يكون محدداً من حيث المحل الذي يرد عليه والأشياء المراد البحث عنها لضبطها، وأن تكون هناك دلائل جدية ومعقولة تُرَجح وقوع الجريمة الصادر بشأنها [1].

وعبر قانون الإجراءات الجنائية الأمريكي عن الدلائل الكافية باصطلاح السبب المعقول أو المحتمل، ونص على ذلك أيضاً التعديل الرابع للدستور الأمريكي، فذكر بأنه لا يجب إصدار أوامر القبض أو التفتيش ما لم تكن بناء على سبب معقول. وفيما يتعلق بالجرائم التي تقع على الوسائل الإليكترونية ويصدر الإذن بالتفتيش لضبط أدلة تفيد في وقوعها فإنه يقصد بالدلائل الكافية بالنسبة لها مجموعة المظاهر والإمارات التي تكفي وفقاً للسياق العقلي والمنطقي أن ترجح ارتكابها ونبتها إلى شخص معين سواء أكان وصفه فاعلاً لها أم شريكاً. وإذا كان الغرض من إذن التفتيش جمع الأدلة بشأن الجريمة التي تكون قد وقعت على الوسائل الإليكترونية أو عن طريق هذه الوسائل فإنه يلزم أن تكشف الإمارات القوية والقرائن على وجود أشياء أو أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة لدى المتهم وترجح ارتكابه للجريمة، ومثال ذلك وجود أدوات تكون قد استعملت في ارتكاب الجريمة أو لضبط أشياء متحصله منها، أو مستندات إليكترونية، أو دعامات تفيد في إماطة اللثام عنها. فالإذن بالتفتيش الذي يقع على الوسائل الإليكترونية قد يصدر لجمع أدلة عن جرائم تكون قد وقعت على البرنامج أو الكيان المنطقي،

---

(1) رستم، هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، المرجع السابق.

أو نظام التشغيل، أو النظم الفرعية، أو البرامج والخدمات المساعدة أياً كان شكلها، أو دعاماتها المادية، أو وعائها، أو على المستندات التي تكون متعلقة بهذا البرنامج أو الكيان المنطقي بما في ذلك البيانات المعدة للتسجيل، أو المسجلة في ذاكرة الحاسب، أو في مخرجاته أياً كانت شكلها، أو دعامتها، أو وعائها، أو على السجلات المثبتة لاستخدام نظام المعالجة الآلية للبيانات أياً كان شكل هذه السجلات، أو الدعامة المادية التي تُجسدها، أو على السجلات الخاصة بعمليات دخول نظم المعالجة الآلية للبيانات كسجلات كلمات السر ومفاتيح الدخول، ومفاتيح فك الشفرة أياً كان شكلها، أو دعامتها، أو وعائها. وبالنظر إلى الطبيعة الفنية للجرائم التي قد تقع على الوسائل الإليكترونية فإنه يمكن الاستعانة في ذلك بمأموري الضبط ذوي الخبرة الفنية في هذا المجال بما يساعد في جمع الدليل بشأن هذا النوع من الجرائم. وقد يدق الأمر بالنسبة للتفتيش الوسائل الإليكترونية إذ قد يحتاج الأمر إلى معرفة كلمات السر، أو مفاتيح الشفرة التي تمكّن من الدخول إلى نظمها والاطلاع على محتوياتها [1].

الفرع الأوّل

التزام المتهم بإفشاء أسرار الوسائل المعلوماتية

مما لا شك فيه أن المتهم يتمتع عبر مراحل الدعوى الجنائية بالحماية المقررة له بموجب مبدأ وجوب افتراض براءته إلا أن يثبت العكس بالحكم الجنائي البات. ويترتب على ذلك أنه لا يجوز إجباره على تقديم دليل يدين به نفسه، بل له الحق في الصمت إلا إذا كان كلامه دفاعاً عنه. ويجب ألا يفسر صمته بأنه إقرار منه بصحة الاتهام المنسوب إليه. ويترتب على ذلك أنه لا

(1) علي، عبد الصبور عبد القوي، الجريمة الإليكترونية، المرجع السابق.

يجوز إجبار المتهم على كشف مفاتيح الدخول إلى نظم الوسائل الإليكترونية أو طباعة ملفات بيانات مخزَّنة داخل هذه النظم [1].

وأما بالنسبة لأشخاص آخرين لم يصدر قبلهم الإذن بالتفتيش فهؤلاء الأشخاص الذين يتعاملون مع الوسائل الإليكترونية بحكم طبيعة عملهم لا يعتبرون بمطلق القول شهوداً وفقاً لمدلول الشهادة كدليل إثبات في المواد الجنائية، والتي يقصد بها المعلومات الصادرة من شهود يكونون قد شاهدوا بأبصارهم الجريمة لحظة وقوعها أو قد تجمعت لديهم أدلة تفيد في إثبات وقوعها. أما الشاهد بالنسبة للجرائم التي تقع في محيط الوسائل الإليكترونية فيقصد به صاحب الخبرة والتخصص في تقنية وعلوم الحاسب والذي تكون لديه معلومات جوهرية لازمة لإمكان الدخول في نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة بداخلها. ويعد من هؤلاء الشهود: مشغلو الحاسبات، خبراء البرمجة، المحللون، مهندسو الصيانة والاتصالات ومديرو النظم. وتفرض بعض التشريعات المقارنة التزاماً قانونياً بالإدلاء أو بالإفصاح عن الشفرات، وكلمات السر، أو المرور التي تلزم للدخول إلى نظم الحاسبات الآلية وذلك من خلال التزامه بالإجابة على الأسئلة التي تتعلق بها، ويقع عليه كذلك واجب المعاونة في طبع واستنساخ ما قد تستلزمه مصلحة التحقيق من ملفات بيانات مخزَّنة في ذاكرة الحاسب. فالمشرِّع الإجرائي الفرنسي يلزم الشهود الذين يقع عليهم التزام قانوني بأداء الشهادة بالكشف عن الأكواد وكلمات السر بالنسبة للحاسبات الآلية، ولا يعفيهم من هذا الالتزام إلا التمسك باحترام السر المهني. وعلى ضوء ذلك يمكن القول بأن الشاهد يلتزم بالنسبة للجرائم التي تقع في محيط الوسائل الإليكترونية بطبع ملفات البيانات المخزنة في ذاكرة الحاسب أو حاملات البيانات الثانوية، وأن يفصح عن كلمات المرور السرية وعن أكواد الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج المختلفة. ولا شك في أن وجود

---

(1) أحمد، هلالي عبد اللاه، التزام الشاهد بالإعلام في الجرائم المعلوماتية، دراسة مقارنة، النسر الذهبي، القاهرة، 2000م.

الالتزام القانوني الذي بموجبه يمكن مطالبة المهنيين والحرفيين من الشهود ومستخدمي الوسائل الإليكترونية بالإعلام عن المعلومات والبيانات الجوهرية التي في حوزتهم، ليُمثل أهمية عظيمة في إمكانية جمع الأدلة التي ترتكب على هذه الوسائل، وأنه يلعب دوراً وقائياً هاماً إذ أن تطبيقه يمنع من ضبط النظام الشبكي بأكمله وعدم عزله عن البيئة المعلوماتية المحيطة به. ولعل الطبيعة الخاصة بالجرائم التي تقع في محيط الوسائل الإليكترونية تتطلب تأهيلاً فنياً خاصة بالنسبة لمأموري الضبط القضائي الذين يُناط بهم ضبط هذه الجرائم وجمع الأدلة بشأنها وذلك لكي يمكنهم التعامل السليم مع مخرجات هذه الوسائل ومع دعائمها وبرامجها للحفاظ على سلامة الأدلة المتحصلة عنها من كل تلف أو مسح [1].

---

(1) عرب، يونس، قانون الكمبيوتر، موسوعة القانون وتقنية المعلومات، المرجع السابق.

الفصل الخامس

الخبرة والمعاينة في الجرائم المعلوماتية

مقدمة:

تُعتبر كل من الخبرة والمعاينة أكبر العقبات التي تواجه الإثبات في الجرائم المعلوماتية، فالمعاينة إجراء بمقتضاه ينتقل المحقّق إلى مكان وقوع الجريمة ليشاهد آثارها بنفسه، فيقوم بجمعها وجمع أي شيء يفيد في كشف الحقيقة، وتقتضي المعاينة إثبات حالة الأشخاص والأشياء الموجودة بمكان الجريمة ورفع الآثار المتعلقة بها كالبصمات والدماء وغيرها مما يُفيد التحقيق، والمعاينة تكون شخصية إذا تعلّقت بشخص المجني عليه، أو إمكانية إذا تعلّقت بالمكان الذي تمت فيه الجريمة، ووضع الشهود والمتهم والمجني عليه، أما المعاينة العينية فهي التي تتعلق بالأشياء أو الأدوات المستخدمة في ارتكاب الجريمة وقد يقتضي الأمر الاستعانة بخبير للتعرُّف على طبيعة المادة أو نوعها إذا كان ذلك يحتاج لرأي المتخصص، وفي هذه الحالة يتم إرسال هذه الأشياء إلى الخبير لنكون أمام بصدد إجراء آخر من إجراءات التحقيق وهو الخبرة، فالخبرة هي أحد أهم وسائل جمع الأدلة، يلجأ إليها المحقّق عند وجود واقعة مادية أو شيء مادي يحتاج التعرف عليه إلى حكم الخبير المتخصص، فهو يأخذ حكم الشاهد من حيث الحجية أو القوة في الإثبات[1].

(1) أحمد، هلالي عبد اللاه، التزام الشاهد بالإعلام في الجرائم المعلوماتية، دراسة مقارنة، النسر الذهبي، القاهرة، 2000م.

ولو نظرنا إلى السلوك الإجرامي في الجريمة المعلوماتية عبارة عن بيانات مخزّنة في نظام معلوماتي يتطلب إثباته انتقال محقق متخصص حيث يتم التفتيش عن البيانات عن طريق نقل محتويات الاسطوانة الصلبة الخاصة بالجهاز، ويجب على المحقق أو ضباط الشرطة المتخصصين استخراج المعلومات التي من شأنها أن تساعد التحقيق وأن يطلعوا زملائهم عليها، مثل القيام بالبحث في بنوك المعلومات وفحص كل الوثائق المحفوظة ومراسلات مرتكب الجريمة مثل الرسائل الإليكترونية، وفك شفرات الرسائل المشفرة. وهو ما يحدث عندما ترتكب الجريمة عبر شبكة الانترنت، ولكي ينجح المحققون في عملهم يجب أن يقتفوا أثر الاتصالات منذ الحاسب المصدر إلى الحاسب أو المعدات الأخرى التي تملكها الضحية، مروراً بمؤدي الخدمة والوساطة في كل ودولة. كما يقتضي ذلك أيضاً أن يعمل المحقق على الوصول إلى الملفات التاريخية التي تُبين لحظات مختلف الاتصالات. من أين صدرت؟ ومن الذي يحتمل إجراؤها، بالإضافة إلى ضرورة إلمام المحقق بالحالات التي يكون عليه فيها التحفظ على الجهاز أو الاكتفاء بأخذ نسخة من الاسطوانة الصلبة للحاسب، والأوقات التي يستخدم فيها برامج استعادة المعلومات التي تم إلغاؤها (1)

فالمحقق الذي يقوم بمعاينة الجريمة المعلوماتية يجب أن يكون ملماً بمهارات هذه التقنية، مثل القدرة على استخدام براج Time stamp وهي البرامج التي يمكن عن طريقها تحديد الزمن الذي تم فيه السلوك الإجرامي، لأن ذلك لا يكون متاحاً في جميع الأنظمة المعلوماتية، أما الخبير ففي هذه الحالة يجب أن يكون ملماً بمهارات تحليل البيانات ومهارات التشفير

---

(1) Recommandations sur le dépistage des communications électroniques transfrontalière dans le cadre des enquêtes sur les activités criminelles www G8 Mont tremblant Canada 21 mai 2002.

التي تتيح له فك الرموز استعادة البيانات الملغية cryptanalysis skills [1].

ولما كانت الجرائم تُرتكب عبر الشبكة الدولية فقد نصت المادة 23 على أن: (تتعاون كل الأطراف، وفقاً لنصوص هذا الفصل، على تطبيق الوسائل الدولية الملائمة بالنسبة للتعاون الدولي في المجال الجنائي والترتيبات التي تستند إلى تشريعات موحدة ومتبادلة وكذلك بالنسبة للقانون المحلي على أوسع نطاق ممكن بين بعضهم البعض بغرض التحقيقات والإجراءات المتعلقة بالجرائم الجنائية للشبكات والبيانات المعلوماتية، وكذلك بشأن الحصول على الأدلة في الشكل الإليكتروني لمثل هذه الجرائم)، كما نصت المادة 30 من الاتفاقية على الكشف السريع عن البيانات المحفوظة حيث نصت على:« أنه عند تنفيذ طلب حفظ البيانات المتعلقة بالتجارة غير المشروعة والمتعلقة باتصال خاص تطبيقاً لما هو وارد في المادة 29 فإن الطرف المساند إذا اكتشف وجود مؤدي خدمة في بلد آخر قد شارك في نقل هذا الاتصال فإن عليه أن يكشف على وجه السرعة إلى الطرف طالب المساعدة كمية كافية من البيانات المتعلقة بالتجارة غير المشروعة حتى يمكن تحديد هوية مؤدي الخدمة هذا والطريق الذي تم الاتصال من خلاله». كما أشارت المادة 31 إلى المساعدة المتعلقة بالدخول إلى البيانات المحفوظة. حيث أجازت لأي طرف أن يطلب من أي طرف آخر أن يقوم بالتفتيش ،أو أن يدخل بأي طريقة مشابهة وأن يضبط، أو يحصل بطريقة مماثلة، وأن يكشف عن البيانات المحفوظة بواسطة شبكة المعلومات داخل النطاق المكاني لذلك الطرف والتي يدخل فيها أيضاً البيانات المحفوظة وفقاً للمادة 29من الاتفاقية [2].

---

(1) البربري، صالح أحمد، دور الشرطة في مكافحة جرائم الانترنت في إطار الاتفاقية الأوروبية، الموقعة في بودابست في 2001/11/23م، www. arablawinfo. com

(2) أحمد، هلالي عبد اللاه، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية (على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001م، الطبعة الأولى، دار النهضة العربية، القاهرة، 2006م.

فالخبرة والمعاينة الجنائية في الجرائم المعلوماتية اليوم تحتاج إلى إدارة خاصة يعمل بها متخصصون في أنظمة المعلومات ويتمتعون بصفة الضبطية القضائية، وهو ما يتطلب إنشاء إدارة خاصة للخبرة والمعاينة في الجرائم المعلوماتية، ولا يجب الاكتفاء بمجرد تدريب القائمين على إدارة الخبرة الجنائية، أما رجال القضاء والنيابة والضبطية القضائية فلا شك أنهم يحتاجون للتدريب على استخدام مهارات الحاسب لآلي والموسوعات القانونية التي تتطلب ربط كافة المؤسسات القضائية بقواعد بيانات قانونية مثل أحكام المحاكم والقوانين المختلفة، لتوفير إمكانية استخدام موسوعات القوانين ومجموعات الأحكام القانونية العربية المختلفة وتعليمات النائب العام، لرفع مستوى الكفاءة القانونية لدى رجال القضاء والنيابة العامة (1).

فمع تطور وسائل التحقيق الجنائي في عصر المعلوماتية تطوراً ملموساً يواكب حركة الجريمة وتطور أساليب ارتكابها، فبعد أن كان الطابع المميز لوسائل التحقيق العنف والتعذيب للوصول إلى الدليل، أصبحت المرحلة العلمية الحديثة القائمة على الاستعانة بالأساليب العلمية واستخدام شبكة الإنترنت هي الصفة المميزة والغالبة.

ومرد ذلك حدوث طفرة علمية في مجال تكنولوجيا المعلومات والاتصالات واستخدام الوسائط الإليكترونية في شتى مجالات الحياة، فكلما اكتشف العلم شيئاً حديثاً وجد هذا الاكتشاف طريقه إلى مجال الإثبات الجنائي والتدليل(2).

ولا شك ظهور أنماط جديدة من الجرائم لم تكن مألوفة من السابق –

(1) رستم، هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، المرجع السابق.

(2) بيومي، حجازي عبد الفتاح، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دراسة متعمقة في جرائم الحاسب الآلي والانترنت، دار الكتب القانونية، القاهرة، 2002م.

ونحن لا نزال في بداية عصر الانفجار المعلوماتي - يعني توقع ظهور المزيد والمزيد من هذه الأنماط الجديدة، والذي يتوجب معها تحديث الأنظمة والتعليمات والجهات الأمنية المختصة بمعالجة القضايا الناتجة عن ظهور هذه الأنماط الجديدة، وهو ما يستتبع تطوير أسلوب التحقيق فيها [1].

---

(1) رستم، هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، المرجع السابق.

القسم الأوّل

الخبرة في الجرائم المعلوماتية

المبحث الأوّل

مفهوم الخبرة ومجالاتها في الجرائم المعلوماتية

المطلب الأوّل

مفهوم الخبرة

الخبرة هي: بحث لمسائل مادية أو فنية يصعب على المحقّق أن يشق طريقه فيها ويعجز عن جمع الأدلة بالنسبة لها بالوسائل الأخرى للإثبات، كفحص بصمات عثر عليها بمكان الحادث، أو مدى نسبة توقيع معين إلى شخص بعينه، أو تحديد سبب الوفاة في جريمة قتل عمد، ولأجل الوقوف على الحقيقة في مثل هذه المسائل العلمية والفنية فإن المحقّق أجاز له القانون أن يستعين بخبير متخصص في المسألة موضوع الخبرة، ويُعد ندب المحقق للخبير إجراء من إجراءات التحقيق يقطع التقادم، وذات الشأن بالنسبة لإيداع تقرير الخبرة، لكن أعمال الخبرة ذاتها لا اثر لها على التقادم لأنها أعمال مادية. وإذا ولينا وجهنا شطر ثورة الاتصالات عن بعد نجد أنها قد أتت بتقنيات علمية ذات طبيعة فنية متقدمة، وقد أفرزت هذه التقنيات جرائم ذات طبيعة فنية وعلمية معقدة، يحتاج جمع الدليل بالنسبة لها إلى بحث مسائل علمية وفنية، فالأدلة قد تكون غير مرئية ويلزم تحويلها إلى أدلة مقروءة، وقد تكون نتيجة تلاعب في حسابات معينة، أو في نظم إليكترونية معينة بحيث يحتاج الكشف عنها إلى متخصصين لإثبات هذا التلاعب. وقد

يحتاج الأمر إلى عمليات فنية دقيقة لإمكان الدخول إلى أنظمة الوسائل المعلوماتية نتيجة استخدام الشفرات والأكواد السرية. وإذا كان الهدف من الخبرة الوصول إلى الحقيقة في مسائل علمية وفنية ومادية، فإنها لا تكون حكراً على سلطة التحقيق وإنما يحقُّ للمحكمة أن تأمر بها [1].

وبالنظر إلى الطبيعة الخاصة بالجرائم المعلوماتية، فإن إماطة اللثام عنها قد يحتاج إلى خبرة فنية قد تظهر الحاجة إليها منذ بدء مرحلة التحري عن هذه الجرائم، ثم تستمر الحاجة إليها في مَرحلتي التحقيق والمحاكمة نظراً للطابع الفني الخاص بأساليب ارتكابها والطبيعة المعنوية لمحل الاعتداء[2].

المطلب الثاني

مجالات الخبرة الجرائم المعلوماتية

تتنوّع العمليات المعلوماتية باستخدام الوسائل المعلوماتية، فنجد أمثلة لها في الأعمال المصرفية، وفي الإدارة المعلوماتية، وفي التجارة الإليكترونية، ولذلك فإنه يتصور تنويع الجرائم التي تقع على هذه العمليات وفقاً لنوع الوسائل المعلوماتية المستخدمة في ارتكابها، ومن أمثلة تلك الجرائم ما يلي[3]:

---

(1) بيومي، حجازي عبد الفتاح، صراع الكمبيوتر والانترنت، في القانون العربي النموذجي، دار الكتب القانونية، القاهرة، 2007م.

(2) احمد، هلالي عبد اللاه، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية (على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر)، المرجع السابق.

(3) البداينة، ذياب. (1999م). التطبيقات الاجتماعية للانترنت، ورقة قدمت في الدورة التدريبية حول شبكة الانترنت من منظور أمني، أكاديمية نايف العربية للعلوم الأمنية، بيروت – لبنان.

1 - تزوير المستندات المدخَلة في أنظمة الحاسبات الآلية أو الناتجة بعد المعالجة.

2 - التلاعب في البيانات.

3 - الغش أثناء نقل وبث البيانات.

4 - التلاعب في البرامج الأساسية أو برامج التطبيقات.

5 - سرقة البيانات والمعلومات المعلوماتية.

6 - الدخول غير المشروع للبيانات المعلوماتية.

ولا شك في أن طبيعة هذه الجرائم تستوجب توافر شروط خاصة في الخبير الذي ينتدب لبحث مسائل فنية وعلمية بالنسبة لها.

المبحث الثاني

شروط الخبرة في مجال الجرائم المعلوماتية

إذا كانت الوسائل المعلوماتية متعددة وأن شبكات الاتصال بينها متنوعة، كما وأن طبيعتها الفنية تجعلها موزّعة على تخصصات فنية وعلمية دقيقة، فإن ذلك يستوجب من جهات التحقيق والمحاكمة أن تراعي ذلك عند اختيارها للخبير، فيجب أن تتيقّن أنه تتوافر لديه الإمكانات والقدرات العلمية والفنية في مجال التخصص الدقيق للحقل الذي يطلب منه بحثه، ولا يكفي في ذلك حصول الخبير على درجة علمية معينة، وإنما يجب أن تتوافر لديه أيضا الخبرة العلمية التي تُمكنه من اكتساب كفاءة فنية عالية. وبالنظر إلى الطبيعة الفنية والعلمية للخبرة في مجال الجرائم المعلوماتية، فإنه يمكن تحديد هذه الخبرة في الموضوعات الآتية:

1 - قدرة الخبير على إتقان مأموريته دون أن يترتب على ذلك إعطاب أو تدمير الأدلة المتحصلة من الوسائل الإليكترونية.

2 - طبيعة البيئة التي يعمل في ظلها الحاسب من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية، وتحديد أماكن التخزين والوسائل المستخدمة في ذلك.

3 - الإلمام بتركيب الحاسب وصناعته وطرازه ونظم تشغيله الرئيسة والفرعية، والأجهزة الطرفية الملحَقة به، وكلمات المرور أو السر وأكواد التشفير.

4 - التمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدلة مقروءة، أو المحافظة على دعاماتها لحين القيام بأعمال الخبرة بغير أن يلحقها تدمير أو إتلاف، مع إثبات أن المخرجات الورقية لهذه الأدلة تطابق ما هو مسجّل على دعائمها الممغنطة.

وتجدر الإشارة إلى أنه وإن كان من المقرر أن المحكمة تملك سلطة تقديرية بالنسبة لتقدير الخبير الذي يرد إليها، إلا أن ذلك لا يمتد إلى المسائل الفنية، فلا يجوز لها تفنيدها إلا بأسانيد فنية. تخضع للتقدير المطلق لمحكمة الموضوع، ومن ثم فلا تستطيع المحكمة أن تُفندها وترد عليها إلا بأسانيد فنية قد يصعب عليها أن تشق طريقها فيها إلا عن طريق خبرة فنية أخرى [1]، وان كان حديثنا عن موضوعات الخبرة يتطلب التعرُّض للضبط في العناصر التالية.

المطلب الأوّل

ضبط الأدلة المتحصلة من الوسائل المعلوماتية

لكي يُحقق التفتيش هدفه في جمع الأدلة عن الجريمة التي ارتُكبت فلا بد من إيجاد وسيلة بموجبها يتم وضع اليد على شيء يتصل بها، ويفيد في كشف الحقيقة عنها وعن مرتكبها، وهذه الوسيلة تتمثَّل في الضبط والتي عن طريقها يتم الوصول إلى الأدلة التي تهدف إليها إجراءات الإثبات الجنائي[2].

والضبط بالنسبة للجرائم التي تقع على الوسائل المعلوماتية أو عن طريقها يشتمل على كل ما استعمل في ارتكابها أو أُعد لهذا الغرض، كأجهزة نسخ وتسجيل برامج الحاسب الآلي، أجهزة ربط مع الشبكات الإليكترونية بما يُسمى Modem، أجهزة اختراق الاتصالات وتحليل الشفرات وكلمات

(1) تمام أحمد حسام طه، الجرائم الناشئة عن استخدام الحاسوب، (الحماية للحاسوب)، دراسة مقارنة، المرجع السابق.

(2) بيومي، حجازي عبد الفتاح، صراع الكمبيوتر والانترنت، في القانون العربي النموذجي، المرجع السابق.

السر، كافة البرامج المقلدة والمنسوخة، جميع أوراق النقد المزورة، المحررات المعلوماتية المزورة، التوقيعات المعلوماتية المزورة والملفات المعنوية التي تعد وسيلة لارتكاب الجريمة.

والضبط هنا يُقصد به الضبط القضائي والذي يستهدف الحصول على دليل لمصلحة التحقيق عن طريق إثبات واقعة معينة. والضبط قد يقع على مكوّنات الوسائل الإليكترونية وقد يكون محله أيضاً المراسلات المعلوماتية.

الفرع الأوّل

ضبط الوسائل المعلوماتية في الجرائم المعلوماتية

هناك جانباً من الفقه قد ذهب إلى صلاحية هذه المكوّنات كمحل يقع عليه التفتيش. وهو تأييد خضوع الكيانات المعنوية لإجراء التفتيش؛ لأن لفظ «شيء» لا ينحصر عند مدلوله الضيق في الكيان المادي، وإنما يُشكل كل ما يدخل في جنسه وفقاً للتفسير المنطقي الذي يفسر النص على ضوء المصلحة التي يُحققها المشرّع من ورائه. ويترتّب على ذلك أن الشيء طالما يحقق منفعة أو مصلحة اقتصادية، فإنه يكون محلاً للحماية سواء أكان هذا الشيء من الكيانات المادية أو المعنوية. فالشيء إذا كان يُمثل قيمة اقتصادية أو ذهنية، فإنه يستحق الحماية الجنائية سواء أكان ذو طبيعة مادية أو معنوية، فليس بشرط أن الشيء لكي تتقرّر حمايته ضد السرقة، مثلاً أن يكون ذو قيمة مالية، فالسرقة تقع حتى ولو كان محلها أشياء ليست ذات قيمة مالية، كسرقة مستندات من قضية، أو سرقة أسرار صناعية أو تجارية. ولذلك نجد أن قضاء محكمة النقض الفرنسية وقبل تجريم المشرّع لسرقة الطاقة بموجب نص المادة 2/311 من قانون العقوبات الفرنسي، ذهب إلى صلاحية التيار الكهربائي لقيام جريمة السرقة، وأيضاً يمكن أن تقوم جريمة

السرقة عن طريق الكمبيوتر. وأيضاً فقد ذهبت محكمة النقض المصرية إلى أن جريمة السرقة يمكن أن تقع على سرقة التيار الكهربائي، ويمكن أيضاً أن تقع على خط التليفون. كما وأن فعل الاختلاس يمكن أن يقع على الأشياء المعنوية طالما كانت قابلة للتحديد كالمعلومات التي تحتويها دعامات مادية كالكتابة وشرائط التسجيل المغناطيسية [1]. وفي هذا المعنى قضت محكمة النقض الفرنسية بأن: «سرقة الأقراص المغناطيسية، الديسكات» يتضمَّن في الوقت ذاته سرقة محتوياتها المعلوماتية للفترة الزمنية التي تكون محمَّلة بها.

وبناء على ذلك فإن ضبط الأدلة المتحصلة من التفتيش يمكن أن يقع على الكيانات المعنوية في الوسائل المعلوماتية، ومثال ذلك أنه يمكن ضبط البيانات المعلوماتية أو قاعدة البيانات بمشتملاتها من ملفات، وسجلات، وحقول، وسواء اتخذت برامج نظام أو برامج تطبيقات. فإذا كان التفتيش ينتهي بتحديد موضع ومكان البيانات التي يستهدف الوصول إليها، فإن المعالجة التي تجري عليها لجعلها مرئية للاطلاع عليها وإثباتها، أو بإخراجها من الحاسب في صورة مستندات مطبوعة لا تُعد تفتيشاً عن أدلة الجريمة، ولكنها تُمثل وصولاً إلى هذه الأدلة ومن ثم تُعد ضبطاً لها. وتجدر الإشارة إلى أن ضبط الأدلة المتحصلة من الوسائل الإليكترونية قد تكتنفه الصعوبة البالغة عندما يكون متعلقاً بنظام آلي بأكمله، إذ أن هذا الأمر يحتاج إلى تعاون دولي لأجل إتمام هذا الضبط دون إعاقة سير النظام المعلوماتي. وأما بالنسبة للمكوّنات المادية للحاسب الآلي، فلا يُثير ضبطها أي مشكلات، فيمكن ضبط الوحدات المعلوماتية الآتية: وحدة المدخلات بما تشمله من مفردات كلوحة المفاتيح وشاشة اللمس، نظم الإدخال المرئي، نظام الإدخال الصوتي، نظام الفأرة، نظام القلم الضوئي، نظام القراءة الضوئية للحروف، نظام قراءة الحروف المغناطيسية ونظام إدخال الأشكال والرسومات. ويمكن أيضاً ضبط وحدة الذاكرة الرئيسة سواء أكانت ذاكرة للقراءة فقط أم كانت

---

(1) مندورة، محمد محمود، الجرائم الحاسب الآلية، دورة فيروس الحاسب الآلي، المرجع السابق.

للقراءة والكتابة معاً، وضبط وحدة الحساب والمنطق بما تشمله من دائرة إليكترونية ومسجلات، وضبط وحدة التحكم، وضبط وحدة المخرجات وما تشتمل عليه من وسائل كالشاشة، الطابعة، الرسم والمصغرات الفيلمية، وضبط وحدات التخزين الثانوية بما تشمل عليه من أقراص مغناطيسية بنوعيها المرن والصلب والأشرطة المغناطيسية. ويُلاحظ كذلك أنه يمكن ضبط كافة الأدوات والمستندات التي تكون قد استُعملت، أو تحصلت من الجرائم التي تقع على العمليات الإليكترونية، فيمكن ضبط الأوراق المالية المزورة، وقد تضبط هذه الأوراق بداخل الحاسبات الآلية، أو تضبط أدواتها بداخل نظم الحاسب كالأوراق المعدَّلة لذلك والأشرطة المغناطيسية وغير ذلك من وسائل التزوير، ويمكن أيضاً ضبط المحررات الإليكترونية المزورة كمخرجات أو بيانات داخل ذاكرة الحاسب الآلي، ويمكن كذلك ضبط عمليات الغش والنصب التي تتم بالنسبة لأنظمة الصرف الآلي للنقود طبقاً لما هو مسجَّل من بيانات حقيقية داخل هذه الأنظمة. وأيضاً فإن الضبط قد يشمل الأشياء التي تكون قد تعرَّضت للتخزين أو للإتلاف على النحو الذي تكشف عنه الكيانات المادية والمنطقية للحاسبات الآلية[1].

الفرع الثاني

ضبط المراسلات الإليكترونية

على الرغم من أن ثورة المعلومات قد أسعدت الأفراد بما وفرته لهم من سبل الاتصال الحديثة والتي انعكس أثرها على مختلف مناحي حياتهم، إلا إنها قد سبَّبت لهم الكثير من الأضرار شخصية، ليس فقط فيما يتعلَّق

(1) رستم، هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، المرجع السابق.

بالجرائم المستحدَثة التي قد تُرتكب ضدهم، وإنما كذلك بالنسبة لانتهاك أسرارهم الشخصية عن طريق الوسائل الإليكترونية المتقدمة. ونظراً لصلة المراسلات بالحياة الخاصة للأفراد، نجد أن الدستور المصري قد اتفق مع الدساتير الأخرى وأنزل حماية دستورية على هذه المراسلات، وعلى هدي هذه الحماية الدستورية نجد أن المشرِّع الإجرائي قد قيَّد سلطة التحقيق في ضبط المراسلات بأنواعها المختلفة، فاشترط لذلك أن يكون إجراء الضبط مفيداً في ظهور الحقيقة وأن تكون الجريمة التي تتطلب اتخاذه جناية أو جنحة معاقَب عليها بالحبس لمدة تزيد على ثلاثة أشهر، وحدد المدة الزمنية لإجراء الأمر بالمراقبة لمدة لا تزيد على ثلاثين يوماً، واستلزم تسبيب هذا الأمر. وإذا كانت النيابة العامة هي الآمرة به فألزمها بأن تحصل مقدمها على أمر مسبَّب بذلك من القاضي الجزائي المختص ولمدة لا تزيد أيضاً على ثلاثين يوماً، ويجوز للقاضي الجزائي أن يُجدد هذا الأمر مدة أو مدداً أخرى مماثلة. ولقد تدخَّل المشرِّع الفرنسي بإصدار القانون رقم 91 – 649 في 10 يوليه 1991م بشأن المراقبة القضائية للاتصالات التليفونية ونص على حرمة المراسلات التي يتم نقلها بطريق الهاتف أو غيره من وسائل الاتصال فلم يجد الرقابة عليها إلا عن طريق السلطة العامة وفي حالات الضرورة التي تُبررها المصلحة العامة المبينة في القانون. والمختص بإصدار قرار المراقبة هي قاضي التحقيق (المادة 1/110) وله أن يندب مأمور الضبط القضائي للقيام به. ولا يأذن بالمراقبة إلا إذا كانت هناك ضرورة تستوجبها ظروف كشف الحقيقة وكانت هناك استحالة في الوصول إليها بطرق البحث والتنقيب العادية (م1/100). وتطلَّب هذا القانون كذلك في الجريمة المراد ضبطها بهذه الوسيلة أن تكون جناية أو جنحة معاقَب عليها بالحبس الذي يزيد عن سنتين (م 2/100) وكذلك حدَّد ميعاداً زمنياً للمراقبة مدته أربعة أشهر في حدِّها الأقصى وتكون قابلة للتجديد. وأنه يتعين أن يتم التسجيل وتفريغ التسجيل تحت سلطة قاضي التحقيق ورقابته (م 100). ولا مرية أن الحماية التي يكفلها المشرِّع للمراسلات العادية لا يقتصر نطاقها على الصور

المختلفة لهذه المراسلات، وإنما منطق القول يُحتم امتداد هذه الحماية إلى المراسلات الإليكترونية من باب أولى بحسبان أن الغاية من وراء هذه الحماية هي حماية الحياة الخاصة للإنسان بحماية مستودع أسراره الشخصية، وهذه الأسرار الشخصية تكون أكثر انتهاكاً إذا ما استخدمت الوسائل الإليكترونية في الوصول إليها، ومن ثم فإنها تكون في حاجة إلى حماية أكثر من تلك الحماية التي تحتاجها المراسلات في صورتها التقليدية. وبناءً على ذلك فإن الحماية التي يُقررها الدستور والمشرِّع العادي للمراسلات العادية تمتد إلى سائر صور المراسلات الإليكترونية المستحدثة كالتراسل باستخدام أجهزة «الفاكسيمل» الناقلة للنصوص والأشكال والرسومات طبقاً لأصولها أو باستخدام «البريد الإليكتروني»، أو بغيرهما من الوسائل التي قد يكشف عنها العلم في المستقبل، طالما كانت هذه الأجهزة أو الأنظمة تابعة لهيئة البريد أو متعهَّد تعهَّد إليه بذلك، وكان موضوع الضبط، أو المراقبة، أو الاطلاع تسجيلات إليكترونية محفوظة لمراسلات تمت، أو مراسلات تبث عبرها. وسنبين فيما يلي ضبط المراسلات الإليكترونية بالنسبة للبريد الإليكتروني، والتصنت والمراقبة الإليكترونية لشبكات الحاسب الآلي[1].

الفرع الثالث

ضبط مراسلات البريد الإليكتروني

يُقصد بالبريد الإليكتروني استخدام شبكات الانترنت في نقل الرسائل بدل من الوسائل التقليدية. وبالنظر إلى سهولة استخدامه فقد أصبح من أكثر وسائل الانترنت شيوعاً واستخداماً في الوقت الحالي. ولعل من الأمور

(1) بيومي، حجازي عبد الفتاح، صراع الكمبيوتر والانترنت، في القانون العربي النموذجي، المرجع السابق.

الهامة التي تتعلق بالبريد الإليكتروني وجوب المحافظة على سريته، وهو ما حدا بالمبتكرين لبرامجه بابتكار برامج تشفير خاصة به بحيث لا يمكن الاطلاع على أي رسالة إلا لمن يعرف هذه الشفرة، ويمكن حفظ البريد الإليكتروني في صناديق بريد خاصة أو في ملف، أو نسخ الرسالة والاحتفاظ بها. ولقد ساعد ظهور التوقيع الإليكتروني في تسيير عملية التراسل عبر البريد الإليكتروني، فالبرنامج يقوم بتخزين توقيع المستخدم كرمز أو شفرة ويضعه تلقائياً على كل رسالة [1].

وإذا كان مفهوم المستندات قد تغيَّر اليوم فقد حلَّت المستندات الرقمية محل الكثير من الوثائق المطبوعة على الورق، فإن الرسائل الإليكترونية تعد مستندات، فالمستند أصبح مفهومه الذي يتفق مع ثورة الاتصالات عن بعد كل أسلوب به تحدد فكرة معينة أو تعبير محدد من خلال كتابة ورقية، أو كتابة إليكترونية، فالعالم يعيش اليوم – وبحق – عصر الثورة الرقمية، حيث صارت الكلمة والصوت والأشعة والصورة والمعلومات رقمية، حتى ليمكن القول أنه قد صار للأرقام هيمنة كونية. ولقد تم الاعتراف في الكثير من التشريعات للمستندات الإليكترونية بحجيتها في الإثبات وأنها تصلح لأن تكون محلاً يقع عليه التزوير. فإذا كان محتوى المحرر قد أصبح يُعبر عنه بلغة رقمية، فإن هذه اللغة هي التي حلت محل الكتابة، ومن ثم يصلح هذا المحرر الرقمي لتقوم به جريمة التزوير. فالمستند الإليكتروني طالما عبر عن فكرة وكان في الإمكان قراءته وإدراك معناه وفهم مضمونه فإنه يعد محرراً». ومن ثم فإنه يحوز الحجية وفقاً لطبيعة الشخص المنسوب إليه إصداره، ولمن وضع عليه توقيعه الإليكتروني. وتجدر الإشارة إلى أنه بصدور القانون الفرنسي الجديد سنة 1994 فقد ألغيت المادتين 5/462 و6/462 والذي جاء بهما القانون رقم 88/19 الصادر في 1988/1/5م بشأن تجريم غش المعلوماتية، وقد كانت المادة الأولى تنص على تجريم تزوير المستندات المعالجة آلياً، بينما

---

(1) رستم هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، المرجع السابق.

كانت الثانية تجرِّم استعمال هذه المحررات، وقد حلَّت محلهما المادة 441 من الكتاب الرابع من قانون العقوبات، بحيث أضيف إليها تزوير المستندات المعالجة آلياً واستعمالها وأصبح نص هذه المادة بعد تعديلها بأنه يُعد تزويراً: «كل تغيير بطريق الغش للحقيقة في مكتوب، أو في أي دعامة أخرى تحتوي على تعبير عن الفكر»، وهكذا تطورت جريمة التزوير في المعلوماتية من مجرد جريمة تزوير المستندات المعالجة آليا فقط واستعمالها إلى جريمة تزوير المستندات المعلوماتية واستعمالها. ويترتب على اعتبار الرسائل الإليكترونية التي تتم عن طريق البريد الإليكتروني بمثابة رسائل شخصية أنه يجب حمايتها بذات الحماية التي تتمتع بها المراسلات الورقية، ومن ثم فلا يجوز التصنُّت عليها أو الاطلاع على الأسرار التي تحتويها إلا بذات الطرق التي تنص عليها قوانين الإجراءات الجنائية. فلا يستطيع المحقق اختراق صندوق البريد الإليكتروني، أو الدخول على أنظمة الحاسب الآلي المخزنة به الرسائل البريدية الإليكترونية وضبطها إلا عن طريق اتباع الإجراءات المنصوص عليها في القوانين الإجرائية والتي تنظم ذلك على النحو سالف الإشارة إليه [1].

المطلب الثاني

المراقبة الإليكترونية للشبكات المعلوماتية

يُقصد بمراقبة المحادثات التليفونية وتسجيلها أنها تُعد إجراء من إجراءات التحقيق، يُباشر في جناية أو جنحة وقعت، للبحث عن أدلتها ضد شخص قامت تحريات جدية على أنه ضالع في ارتكاب هذه الجريمة، أو لديه أدلة تتعلَّق بها، وأن في مراقبة أحاديثه التليفونية ما يُفيد في إظهار الحقيقة، بعد أن صعب الوصول إليها بوسائل البحث العادية، وكانت الجريمة

(1) منصور، محمد حسن، المسئولية الإليكترونية، المرجع السابق.

على درجة من الجسامة تستأهل اتخاذ هذا الإجراء «الاستثنائي» بأن كانت جناية أو جنحة يُعاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر. ولقد اختلف الفقه في تكييف إجراء المراقبة للمحادثات السلكية واللاسلكية، فذهب رأي إلى أنها تُعد تفتيشاً وبالتالي تخضع لقيوده. واستند في ذلك إلى أن هذه المراقبة تتفق مع التفتيش في أن الهدف منها البحث في وعاء للسر توصلاً إلى السر ذاته وإزاحة ستار الكتمان عنه بغرض ضبط ما يُفيد في الوصول إلى الحقيقة. ولا أهمية هنا لوجود الكيان المادي لوعاء السر فيصح أن يكون مادياً يمكن ضبطه بوضع اليد عليه استقلالاً، ويمكن أن يكون معنوياً يتعذّر ضبطه إلا إذا اندمج في كيان مادي، فالغاية من مراقبة المحادثات التليفونية هي البحث عن دليل معين وهي ذات الغاية من مراقبة المحادثات التليفونية من التفتيش. ولقد ذهب رأي آخر إلى التفرقة بين التفتيش والمراقبة، واعتبر الأوّل إجراء غايته العثور على الأدلة المادية وضبطها بوضع اليد عليها وحبسها لمصلحة العدالة، وأما الثانية فليس لها كيان مادي ملموس وأنها قد تؤدي إلى سماع سر للمتحدث ولكنه قوّلي يسمعه المتحدث ولا يلمس له كياناً، والقول بأن هذا الحديث يندمج في كيان مادي هو أسلاك التليفون أو شريط التسجيل لا يصح أن يفهم منه أن الحديث له كيان مادي يمكن ضبطه، فأسلاك التليفون أو التسجيل ليست هي الدليل ذاته، وما هي إلا وسلية أو أداة لسماع الحديث أو إعادته ويبقى الدليل المستَمَد منها حديثاً غير مادي، حيث لا تتأثر طبيعته بوسيلة أو أداة الحصول عليه [1].

والمشرِّع أفرد أحكاماً خاصة لكل من التفتيش والمراقبة على المراسلات السلكية واللاسلكية نظراً لاختلاف المحل الذي يقع عليه كل منهما، فالأخير يقع على حرمة الحياة الخاصة، بمطلق القول، أما الأول فقد يمس بالمصادفة هذه الحياة الخاصة حتى ولو تم على كيانات معنوية. ولذلك نجد أن المشرِّع قد أحاط المراقبة بضمانات تزيد عن تلك المقررة للتفتيش. فليس معنى أنه

(1) الفيومي، محمد، «مقدمة في علم الحاسابات الإليكترونية والبرمجة بلغة بيسك»، المرجع السابق

يتصور وقوع التفتيش على كيان معنوي وأن المراقبة تتم دائماً على كيانات معنوية أن نسوي بينهما من حيث تأثيرهما على حرمة الحياة الخاصة، فالذي لا شك فيه أن المراقبة تكون أشد وطأة في مساسها بحرمة الحياة الخاصة بما قد لا يتوافر بالنسبة للتفتيش. وانطلاقاً من أهمية حماية الحياة الخاصة نجد أن الدستور والمشرِّع العادي قد كفلا حماية خاصة للمراسلات السلكية واللاسلكية على النحو سالف الإشارة إليه فنظم سبل الرقابة عليها وحدد السلطة التي تملك ذلك والإجراءات التي يلزم اتباعها حيال هذه المراقبة. وإذا كانت شبكات الحاسب الآلي تستخدم خطوط التليفون وتستعين في ذلك بجهاز معدل الموجات «Modem» والذي يستطيع تحويل الإشارات الرقمية المستخدمة بواسطة الحاسب إلى موجات تناظرية تنقل مع الموجات الصوتية خلال خطوط التليفون، وبذلك فإنه يتبين وجود علاقة بين المراسلات التي تتم بالطرق التقليدية وتلك التي تتم بالوسائل الإليكترونية بحيث يمكن القول أن هناك تصنتاً ومراقبة إليكترونية تتم على شبكات الحاسب الآلي. ولذلك فقد أجازت بعض التشريعات هذا التصنت الإليكتروني[1]، فالمشرِّع الفرنسي أجاز بقانون 10 يوليو 1991م سالف الإشارة إليه اعتراض الاتصالات عن بعد بما في ذلك شبكات تبادل المعلومات. وفي هولندا يجوز لقاضي التحقيق أن يأمر بالتصنت على شبكات اتصالات الحاسب إذا كان لغرض ضبط جرائم خطيرة، ويمكن أن تتم المراقبة أيضاً على التلكس والفاكس ونقل البيانات ويمكن القول على ضوء ذلك أن النصوص الحالية في التشريع الإجرائي المصري والخاصة بمراقبة المحادثات التليفونية وتسجيلها تكفي لأن يمتد سلطانها لكي تُطبق على المراقبة المعلوماتية لشبكات الحاسب الآلي وذلك إذا أُضيفت عبارة «بما في ذلك شبكات الحاسب الآلي» إلى كل من المادتين 1/95 و2/206 من قانون الإجراءات الجنائية. ولقد تفادى التشريع الفرنسي الصادر في 10 يوليو 1991م هذا النقص بأن نص على حرمة المراسلات التي يتم نقلها

---

(1) رستم، هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، المرجع السابق.

بطريق الهاتف أو غيره بأي وسيلة من وسائل الاتصال. وبانتهاء الحديث عن إجراءات الحصول على الأدلة من الوسائل المعلوماتية وتحديد الأدلة التي ستتحصل من هذه الطرق كالمخرجات الإليكترونية، والمستندات الإليكترونية والكيانات المادية والمعنوية وأنواع الغش والتزوير والإتلاف والتلاعب الذي قد تكشف عنه هذه الطرق، فإن الباب ينفتح عن تقدير هذه الأدلة في إطار نظرية الإثبات الجنائي [1].

(1) عوض، رمزي رياض، مشروعية الدليل الجنائي في مرحلة المحاكمة وما قبلها، دراسة تحليلية تأصيلية مقارنة، المرجع السابق.

المبحث الثالث

الأدلة الرقمية والإثبات الجنائي في الجرائم المعلوماتية

يُسيطر على الإثبات الجنائي مبدأ حرية القاضي في الاقتناع، فالقاضي الجنائي يستطيع أن يستمد عقيدته من أي دليل يرتاح إليه وجدانه. وهذه الحرية التي يتمتع بها القاضي الجنائي ليست مقررة لكي تتَّسع سلطته من حيث الإدانة أو البراءة، وإنما هي مقررة له بالنظر إلى صعوبة الحصول على الدليل في المواد الجنائية. فاستنباط الحقيقة من هذا الدليل إنما يتم بمعرفة القاضي ومدى قدرته على الوصول إلى الحقيقة وما حباه الله من علم ومدى توافر حاسة القضاء لديه. ولذلك نجد أن القاضي الجنائي يتمتع دائماً بدور إيجابي في الدعوى الجنائية. والقاضي وعلى الرغم من أنه يتمتع بالحرية في تكوين عقيدته إلا أنه يلتزم ببيان الأدلة التي أستمد منها اقتناعه، فليست الحرية أن نطلق له العنان لكي يقتنع بما يحلو له، وإنما هو حر – فقط – في استخلاص الحقيقة من أي مصدر مشروع[1].

المطلب الأوَّل

مشكلات الأدلة الجنائية الرقمية

بالنظر إلى الطبيعة الخاصة التي تتميَّز بها الأدلة المتحصلة من الوسائل المعلوماتية وما قد يُصاحب الحصول عليها من خطوات معقَّدة، فإن قبولها في الإثبات قد يُثير العديد من المشكلات، فكما تعلم أن مستودع هذه

---

(1) بيومي، حجازي عبد الفتاح، صراع الكمبيوتر والانترنت، في القانون العربي النموذجي، المرجع السابق.

الأدلة هو الوسائل المعلوماتية، ولذلك فيمكن التلاعب فيها وتغيير الحقيقة التي يجب أن تُعبر عنها. ولذلك فإن المشكلات التي تُثيرها هذه الأدلة ليس بسبب أنها قد تصلح لتكون طرق إثبات أم لا؟ وإنما المشكلة التي تتعلّق بها تتحدد في: كيف نضمن مصداقية هذه الأدلة وأن تعبر بالفعل عن الحقيقة التي تهدف إليها الدعوى الجنائية.

الفرع الأوّل

دور الوسائل المعلوماتية كأدلة إثبات جنائية

تذهب التشريعات المقارنة إلى قبول مصادر المعلومات الخاصة بالحساب الآلي أو المتحصل عليها من أنظمته مثل مخرجات نظام المعالجة الآلية للبيانات والبيانات المكتوبة على شاشته، والبيانات المسجَّلة على دعائم ممغنطة أو المخزَّنة داخل نظام المعالجة كأدلة يقوم عليها الإثبات الجنائي[1].

وهذه الأدلة المتحصلة من الوسائل المعلوماتية تخضع للسلطة التقديرية للقاضي الجنائي، فإن استراح إليها ضميره ووجدها كافية ومنطقية فيمكنه أن يستمد اقتناعه ويعول عليها في الحكم الذي ينتهي إليه، ولقد أُثيرت في فرنسا مشكلة الإثبات لمحاضر المخالفات التي تتم عن طريق جهاز السينموتر، وانتهى القضاء هناك إلى عدم اعتبار محاضر المخالفات المحررة بإثبات المخالفة حجة بذاتها في الإثبات، وإنما ذهب كل من الفقه والقضاء، إلى أن أي محضر لا تكون له قوة إثباتية إلا إذا أثبت فيه محرره وقائع تدخل في اختصاصه، وأن يكون قد شاهدها أو سمعها أو تحقَّق منها بنفسه، وبناء على ذلك فإن المحضر الذي يُحرره عقب عملية المراقبة الإليكترونية للسيارات لا يصلح دليلاً على

(1) رمضان، مدحت، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، القاهرة، 2000م.

ارتكاب الجريمة، حيث أن محرري المحضر لم يتحققوا بأنفسهم من ارتكاب المخالفة. وإذا كان الضابط الذي يُحرر المخالفة للقيادة بسرعة تزيد عن السرعة المقررة والتي يتم ضبطها عن طريق جهاز الرادار طبقاً لقانون المرور المصري، لا يكون قد شاهد بنفسه المخالفة وإنما قام بتسجيلها فقط عن طريق الإشارة اللاسلكية التي تكون قد وصلت إليه، ولذلك فإن تقرير مخالفة المرور عن هذه المخالفة لا يمكن أن يحل محل محضر جمع الاستدلالات ولا يصلح لأن يكون دليلاً قائما بذاته لإثبات المخالفة. ولذلك يمكن القول بأن المخرجات المتحصّلة من الوسائل المعلوماتية لا تُمثل مشكلة في النظام اللاتيني حيث يسود مبدأ حرية القاضي الجنائي في الاقتناع [1].

والفقه الفرنسي يتناول حجية هذه المخرجات في المواد الجنائية ضمن مسألة قبول الأدلة المتحصّلة عن الآلة أو ما يُسمى بالأدلة العلمية والتي يجب ألا تقبل كطرق إثبات إلا إذا توافرت الشروط المقررة لذلك. ويُثير قبول الأدلة المتحصلة من الوسائل المعلوماتية مشكلات عديدة في ظل القواعد الأنجلو أمريكية للإثبات الجنائي، والتي تعتنق كمبدأ أساسي الإثبات بالشهادة التي تتعلق بالواقعة محل الإثبات. ولذلك فإن قبول المستندات المطبوعة لمخرجات الوسائل الإليكترونية والتي هي عبارة عن إشارات إليكترونية ونبضات ممغنطة، يُمثل مشكلة أمام القضاء في هذا النظام، إذ لا يمكن للمحلفين أو القاضي من مناظرة الأدلة المتولدة منها ووضع أيديهم عليها، وهذا يجعلها بمثابة أدلة ثانوية وليست أصلية. ولقد صدر في إنجلترا قانون للإثبات الجنائي في سنة 1984 م وعمل به بدءً من عام 1986 م وقد نصت المادة 68 منه على أن: «يقبل الإثبات بالمحررات التي تتعلّق بأي غرض من الأغراض إذا توافرت شروط معينة وهي[2]:

1 - أن يكون المحرر عبارة عن سجل أو جزء من سجل يعده الشخص

---

(1) عوض، رمزي رياض، مشروعية الدليل الجنائي في مرحلة المحاكمة وما قبلها، دراسة تحليلية تأصيلية مقارنة، المرجع السابق.

(2) مصلح، يحيى، التجارة على الانترنت، سايمون كولن، نقله إلى العربية، بيت الأفكار الدولية بامريكا 1999م.

بموجب واجب يقع على عاتقه ليثبت فيه معلومات مقدمة إليه من شخص آخر.

2 - يمكن قبول افتراض توافر علمه الشخصي بالأمور المتعلقة بها المعلومات.

3 - الا يكون الشخص التي تستقي منه المعلومات متاح وجوده أو ممكنا تعيينه، أو تتبعه، أو يكون غير متوقع منه تذكر الأمور المتعلقة بالمعلومات.

ولقد نصت المادة 69 من ذات هذا القانون على أن الناتج من الوسائل الإليكترونية لا يقبل كدليل إذا تبيّن وجود سبب معقول يدعو إلى الاعتقاد بأن هذا الناتج غير دقيق أو أن بياناته غير سليمة. ويجب كذلك أن يكون الحاسب الناتج منه المخرج الإليكتروني يعمل بكفاءة وبصورة سليمة، ويلاحظ أن هذه التحفظات الأخيرة لا تُطبق إلا إذا كانت مطبوعات الحاسب دليلاً حقيقياً أو أصلياً، وليس مجرد نقل عن الغير. وتجدر الإشارة إلى أن مخرجات الوسائل الإليكترونية تقبل كوسائل إثبات في الولايات المتحدة الأمريكية وذلك بالنسبة للبرامج والبيانات المخزونة فيها، وبالنسبة للنسخ المستخرَجة من البيانات التي يحتويها الحاسب.

فالأنظمة القانونية المختلفة قد قبلت الأدلة المتحصلة من الوسائل المعلوماتية كأدلة إثبات، وإن كان النظام الأنجلو أمريكي قد أورد الكثير من الشروط لقبولها كأدلة إثبات نظراً لطبيعة هذا النظام والذي يعتمد في الأصل على النظام الاتهامي القائم على مبدأ التواجهية وإعلائه للإثبات بالشهادة وتحقيق الأدلة أمام القضاء. وعلى الرغم من التسليم بصلاحية هذه الأدلة لتكون أدلة إثبات فإنها لا تصلح لتكون معبِّرة عن الحقيقة إلا إذا توافرت لها ذات الشروط التي يجب توافرها في أدلة الإثبات الجنائي بحسبان أنها تنتمي إليها، وسنبين فيما يلي هذه الشروط [1].

---

(1) اليوسف، عبدالله عبدالعزيز (1420هـ). التقنية والجرائم المستحدثة، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية، تونس، تونس (195 - 233).

الفرع الثاني

الشروط الواجب توافرها في مخرجات الوسائل المعلوماتية كدليل إثبات في الجرائم المعلوماتية

إن الأدلة المتحصّلة عن الوسائل المعلوماتية قد توجّس منها كل من القضاء والفقه خيفة من عدم تعبيرها عن الحقيقة نظراً لما يمكن أن تخضع له طرق الحصول عليها من التعرُّض للتزييف والتحريف والأخطاء المتعددة، فإن ذلك قد تطلب وجوب توافر مجموعة من الشروط التي قد تُضفي عليها المصداقية ومن ثم اقترابها نحو الحقيقة وقبولها كأدلة إثبات في المواد الجنائية [1].

أوّلاً: أن تكون هذه الأدلة يقينية:

أي لابد أن تقترب نحو الحقيقة الواقعية قدر المستطاع وأن تبتعد عن الظنون والتخمينات، فلا محل لدحض مبدأ أن الأصل في الإنسان البراءة بالنسبة لهذه الأدلة إلا بتعيين مثله أو أقوى منه، وهذا يقين. ويترتب على ذلك أن كافة مخرجات الوسائل الإليكترونية من مخرجات ورقية أو إليكترونية، أو أقراص مغناطيسية، أو مصغرات فيلمية تخضع لتقدير القاضي الجنائي، ويجب أن يستنتج منها الحقيقة بما يتفق مع اليقين ويبتعد عن الشك والاحتمال[2].

والقاضي يمكنه أن يصل إلى يقينية المخرجات المتقدم ذكرها عن طريق: المعرفة الحسية التي تُدركها الحواس من خلال معاينته لهذه المخرجات وفحصها، وعن طريق المعرفة العقلية عن طريق ما يقوم به من استقراء

---

(1) رمضان، مدحت، جرائم الاعتداء على الأشخاص والانترنت، المرجع السابق.

(2) أحمد، هلالي عبد اللاه، التزام الشاهد بالإعلام في الجرائم المعلوماتية، دراسة مقارنة، المرجع السابق.

واستنتاج ليصل إلى الحقيقة التي يهدُف إليها ويحبب أن يصدر حكمه استناداً إليها.

ثانياً: يتعين مناقشة مخرجات الوسائل المعلوماتية لكي تخضع لمبدأ شفوية المرافعة:

فإذا كانت مخرجات الوسائل الإليكترونية تُعد أدلة إثبات قائمة في أوراق الدعوى التي ينظرها القاضي، فإنه يجب عليه مناقشتها أمام الخصوم. ويترتب على ذلك أن هذه المخرجات سواء كانت مطبوعة أم بيانات معروضة على شاشة الحاسب. أما إن كانت بيانات مدرجة في حاملات، أم اتخذت شكل أشرطة وأقراص ممغنطة، أو ضوئية، أو مصغرات فيلمية، تكون محلاً للمناقشة عند الاعتماد عليها كأدلة أمام المحكمة. فإذا كان القاضي الجنائي يحكم باقتناعه هو وليس باقتناع غيره، فإنه يجب عليه أن يُعيد تحقيق كافة الأدلة القائمة في الأوراق لكي يتمكّن من تكوين اقتناع بقربه نحو الحقيقة الواقعية التي يصبو إليها كل قاضٍ عادل ومجتهد. ويترتب على هذا المبدأ أن القاضي لا يمكنه أن يحكم في الجرائم المعلوماتية استناداً إلى علم شخصي له، أو استناداً إلى رأي للغير، إلا إذا كان الغير من الخبراء وقد ارتاح ضميره إلى التقرير المحرر منه فقرر الاستناد إليه ضمن باقي الأدلة القائمة في أوراق الدعوى المعروضة عليه، بحيث أن الاقتناع الذي يكون قد أصدر حكمه بناء عليه يكون متولداً من عقيدته هو وليس من تقرير الخبير.

ثالثاً: جمهور الفقه الإسلامي إلى أن القاضي لا يجوز له أن يقضي بعلمه الشخصي، لأنه لا يجوز له أن يكون شاهداً في القضية التي يحكم فيها[1].

ثالثاً: مشروعة تلك الوسائل المعلوماتية:

إن الإدانة في أي جريمة التي قد تصلح أن تبنى على دليل أخلاقي،

(1) أحمد، هلالي عبد اللاه، التزام الشاهد بالإعلام في الجرائم المعلوماتية، دراسة مقارنة، المرجع السابق.

وهذا يتطلب أن تكون الأدلة مشروعة أي أن الحصول عليها يكون قد تم وفق قواعد اعليه. والنزاهة واحترام القانون، فمبدأ مشروعية الدليل الجنائي بالنسبة لمخرجات الوسائل الإليكترونية يتطلب ضرورة الاتفاق على إجراءات الحصول على هذه المخرجات بما يتفق والقواعد القانونية والأنظمة الثابتة في وجدان المجتمع المتحضر [1].

ويترتب على ذلك أن إجراءات جمع الأدلة المتحصلة من الوسائل الإليكترونية إذا خالفت القواعد الإجرائية التي تنظم كيفية الحصول عليها، فإنها تكون باطلة ولا تصلح لأن تكون أدلة تُبنىَ عليها الإدانة في المواد الجنائية. فمشروعية الدليل تتطلب صدقه في مضمونه، وأن يكون هذا المضمون قد تم الحصول عليه بطرق مشروعة وتدل على الأمانة والنزاهة من حيث طرق الحصول عليه. ويجب التحوط بالنسبة لشرط شرعية الأدلة المتحصلة من الوسائل التكنولوجية في الحصول على الأدلة؛ لأن هذه الأدلة قد تحتوي على حقيقة علمية تُخالف الحقيقة القضائية التي تتطلب لقبول هذه الحقيقة العلمية أن يكون الوصول إليها قد تم بطرق مشروعة. ومن أمثلة الطرق غير المشروعة التي قد يتم من خلالها الحصول على أدلة تتعلق بالوسائل الإليكترونية، استخدام التعذيب، أو الإكراه المادي، أو المعنوي في مواجهة الجاني الذي يرتكب جريمة إليكترونية لكي يفك شفرة أو يبوح بكلمة السر. ويُعد من قبيل هذه الطرق غير المشروعة أيضا: استخدام التدليس، أو الغش، أو الخديعة في الحصول على الأدلة المتحصلة من الوسائل الإليكترونية.

وفي إيطاليا نصت المادة 191 من قانون سنة 1989 م على: «عدم صلاحية الدليل الباطل للاستعمال». وهذا يُفيد رفض الدليل غير المشروع سواء أكان هذا الدليل ينتمي إلى الأدلة التقليدية أم أنه ينتمي إلى الأدلة المتحصلة من الحاسب الآلي [2].

---

(1) الصغير، جميل عبد الباقي، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، (أجهزة الرادار – الحاسبات الآلية – البصمة الوراثية)، دراسة مقارنة، دار النهضة العربية، القاهرة، 2001م.

(2) Information Warfare Principles and Operations, by Edward Waltz 1998.

تقدير أدلة الإثبات المتحصلة عن الوسائل الإليكترونية في ضوء نظم الأدلة الجنائية:

تتنوَّع نظم الأدلة الجنائية في الإثبات الجنائي، بين التي تأخذ بنظام الأدلة القانونية في الإثبات، وأخرى تعتنق نظام الإثبات الحر القائم على حرية القاضي الجنائي في الاقتناع، وتلك التي تجمع بين النظامين بما يُسمى بالنظام المختلط. ووجه الفرق بين هذه النظم أنه في نظام الأدلة القانونية يتقيَّد القاضي في الإثبات الجنائي بأدلة يُحددها له المشرِّع مقدماً ويقدر له قيمتها في الإثبات، فيتقيد القاضي بأن يستمد اقتناعه من هذه الأدلة دون غيرها. أما في نظام الأدلة الإقناعية فإن القاضي لا يُقيده المشرِّع بأدلة إثبات معينة وإنما يترك له حرية الإثبات وفقاً لسلطته التقديرية في تقدير الدليل: ويترتب على ذلك أن للقاضي الجنائي قبول أي دليل يمكن أن يتولَّد منه إقتناعه، وأنه هو الذي يقدر قدرته في الإثبات على قدر اقتناعه به. وعلى الرغم من سيادة هذا النظام الأخير للإثبات الجنائي في جل التشريعات المقارنة، إلا أن البعض منها قد يُطبق في إثبات بعض الجرائم نظام الأدلة القانونية وذلك عندما ينص المشرِّع على تقييد سلطة القاضي في الإثبات بأدلة معينة. ومثال ذلك إعطاء حجية للمحاضر المحررة في بعض المخالفات بالنسبة لما ورد فيها وقائع إلى أن يثبت العكس، وتقييد سلطة القاضي في إثبات بعض الجرائم بأدلة معينة، ومثال ذلك نص المادة 276 من قانون العقوبات المصري إذ نصت على وسائل إثبات محددة لإثبات جريمة الزنا. وهذه الحجية وتلك القيود التي ترد على حرية القاضي في الاقتناع ليس المقصود منها افتراض ارتكاب المتهم للوقائع التي تنص على إعطائها الحجية، ولكنها تعفي القاضي من إعادة التحقيق فيها، ويظل القاضي يملك سلطة تقدير هذه الأدلة ليستمد منها اقتناعه، ويظل المتهم معتصماً بمبدأ افتراض براءته إلى أن يثبت عكس ذلك بالأدلة الكافية والمنطقية. ويلاحظ كذلك أن نظم القانون العام في كل من إنجلترا والولايات المتحدة الأمريكية تضع تشريعات للإثبات الجنائي، كقانون الإثبات في المواد الجنائية الذي

صدر في إنجلترا عام 1984م وعمل به ابتداء من عام 1986م، فهذا القانون قد نظّم طرق الإثبات بالنسبة لمخرجات الحاسب الآلي كأدلة إثبات في المواد الجنائية، وفي الولايات المتحدة الأمريكية فقد صدرت قوانين في بعض الولايات لتنظيم الإثبات الجنائي، فقد صدر في ولاية كاليفورنيا في عام 1983 م تشريعاً للإثبات، وقد نص هذا التشريع على أن النسخ المستخرجة من البيانات التي يحتويها الحاسب تكون مقبولة بوصفها أفضل الأدلة المتاحة لإثبات هذه البيانات، بل إنه في ولاية «أيواء» صدر قانون للحاسب الآلي في سنة 1984 م نص على أن مخرجات الحاسب الآلي تكون مقبولة كأدلة إثبات بالنسبة للبرامج والبيانات المخزونة فيه. وإذا كان التطور العلمي قد أفرز ثورة الاتصالات عن بعد والتي جاءت للبشرية بتكنولوجيا جديدة نراها في مختلف مناحي الحياة، كالتجارة الإليكترونية، وظهور الحاسبات الآلية، وشبكات الاتصال المختلفة، والإدارة الإليكترونية، والتحويلات المصرفية الإليكترونية، وظهور المستندات الإليكترونية، والنقود الإليكترونية، حتى يمكن القول أننا نعيش اليوم عصر الثورة الرقمية التي حلّت بالنسبة لها الذبذبات والنبضات محل الأوراق والكتابة والتوقيعات التقليدية[1].

المطلب الثاني

الاتصالات عن بعد وأثره في الإثبات الجنائي

مما لا شك فيه أن التطور التقني في الاتصالات عن بعد يزيد من دور الخبرة في المسائل الجنائية، بالنظر إلى أن الكثير من الجرائم التي تُرتكب كنتيجة لهذه الثورة ستقع على مسائل إليكترونية ذات طبيعة فنية معقدة، أو

(1) مصلح، يحيى، التجارة على الانترنت، سايمون كولن، نقله إلى العربية، بيت الأفكار الدولية بأمريكا 1999م.

قد تستخدم هذه الوسائل في ارتكابها، وبالنظر إلى تطور مجالات الخبرة فإنه سوف تتّسع مجالات اللجوء إليها [1]. كذلك فقد توفرت التقنية العلمية طرقاً دقيقة لجمع الأدلة بحيث يمكن أن يساهم العلم في صنع الدليل، بحيث أن هذا الدليل قد يتمتع بقوة علمية يصعب إثبات عكسها. أيضاً فقد يعلو شأن الإثبات بالقرائن كنتيجة لاتساع مجال الإثبات بها نتيجة تطور العلوم، ولقد أصبح هذا الأمر جلياً واضحاً في الإثبات بالبصمة الوراثية، وببصمة الصوت، وبصمة قزحية العين وببصمة الشفاه. فالقضاء قد قبل الإثبات بالأدلة المتحصلة عنها عن طريق الرادار، التصوير، السينمومتر، كاميرات الفيديو، مسجلات الصوت، الوسائل الإليكترونية في التصنت. ولا شك في أن ثورة الاتصالات عن بعد في تأثيرها على طبيعة الجرائم التي تُرتكب كنتيجة لاستخدام تقنيتها العلمية ستزيد من تعقيد الدليل الجنائي وطرق الوصول إليه، بحيث أن ذلك قد يؤثر على الطرق التقليدية للحصول عليه فتعجز عن الوصول إلى الدليل الذي يكفي لإثبات هذا النوع الجديد من الجرائم. وهذا الأمر يتطلب أن يلحق التطور طرق الحصول على الدليل الجنائي بالنسبة لهذه الجرائم المستجدَة لكي يمكن عن طريقها الوصول إليه. كذلك فإنه يُلاحظ أن الكثير من المسائل غير الجنائية التي تدخل عناصر تكوينيه في الجرائم الجنائية ستزداد أهميتها كنتيجة لثورة الاتصالات عن بعد، فهذه المسائل قد تغير مفهومها التقليدي فأصبحنا نسمع اليوم عن الشيكات الإليكترونية، وهذا الأمر سيكون له تأثيره بالنسبة لجريمة الشيك بدون رصيد، ويكون إثباته معتمداً على مسائل فنية لإثبات الشيك كورقة تجارية. وأيضاً فقد ظهرت الكيانات غير المادية التي قد تكون محلاً لجريمة خيانة الأمانة، وهذا الأمر يتطلب البحث في توافر العقد المدني الذي تسلّم الجاني هذا الكيان غير المادي بموجبه، فلكي يتم العقاب على هذه الجريمة في قانون العقوبات المصري «المادة 341» فيجب أن يكون المتهم قد تسلّم المال

---

(1) عبادة، عبادة أحمد، التدمير المتعمد لأنظمة المعلومات الإليكترونية مركز البحوث والدراسات، شرطة دبي بدولة الإمارات العربية المتحدة 2005 م

بعقد من العقود المنصوص عليها في هذه المادة. كذلك فإن الاحتيال الذي تقوم به جريمة النصب، قد تطور كنتيجة لاستخدام التقنية العلمية، وأصبح هذا الاحتيال كثير الوقوع في العمليات الإليكترونية، وبالنظر إلى الطبيعة غير المرئية التي يتم بها فقد يصعب إثباته. وليس بِخافٍ كذلك أن المستندات الورقية كمحل تقع عليه جرائم التزوير قد تغيَّر مفهومها بسبب ثورة الاتصالات عن بعد، فقد ظهرت اليوم المستندات الإليكترونية وأصبحت هذه المستندات تصلح في الكثير من التشريعات لتكون محلاً يقع عليه التزوير[1]. ولا شك في أن ظهور هذه المستندات الرقمية سيغير كثيراً من طرق الإثبات الجنائية بالنسبة للجرائم التي تقع عليها، ذلك أن الطرق التقليدية قد لا تقوى على إثباتها، ومن ثم فإن الأمر يحتاج إلى إثبات جنائي جديد يكون في استطاعته إثبات هذا النوع من التزوير، خاصة بعد أن ظهر التوقيع الإليكتروني، وأصبح يتمتع بحجية في الإثبات في الكثير من التشريعات. وهكذا نرى أن الثورة العلمية في الاتصالات لم تؤثر – فقط – في نوعية الجرائم التي ترتبت عليها وفي نوعية الجناة الذين يرتكبون هذه الجرائم، وإنما أثرت تأثيراً كبيراً على الإثبات الجنائي وعلى طرق هذا الإثبات، بحيث يمكن القول أن طرق الإثبات التقليدية قد أصبحت عقيمة بالنسبة لإثبات الجرائم المعلوماتية، وأن الطرق العلمية والفنية للحصول على الدليل قد أصبحت هي المناسبة لإثبات هذا النوع من الجرائم. وإذا كانت الغلبة بالنسبة لإثبات الجرائم الإليكترونية ستكون للإثبات بالقرائن والخبرة، فإن ذلك سيزيد من أهمية الدليل العلمي في الإثبات الجنائي، وفي ذات الوقت يزيد من أهمية دور القاضي في هذا الإثبات بحيث يظل القاضي متمتعاً بسلطة تقديرية في تقدير هذه الأدلة بحسبان أنها قد لا تكون مؤكَّدة على سبيل القطع، أو قد تكون مجرد إمارات أو دلالات، أو قد يحوطها الشك، فهنا تظهر أهمية هذه السلطة التقديرية

---

(1) بوحويش، عطية عثمان محمد، حجية الدليل الرقمي في إثبات جرائم المعلوماتية، رسالة التخصص العالي (الماجستير)، مقدمة إلى أكاديمية الدراسات العليا – فرع بنغازي، للعلم الجامعي 2009م.

التي يجب أن يظل القاضي متمتعا بها؛ لأنه من خلالها يستطيع إظهار مواطن الضعف في هذه القرائن، ويستطيع كذلك تفسير الشك لصالح المتهم. فلا مرية أن الدليل مهما تقدمت طرقه وعلت قيمته العلمية أو الفنية في الإثبات، فإنه يحتاج إلى قاضٍ يتمتع بسلطة تقديرية؛ لأن هذه السلطة التقديرية تكون لازمة لتنقية الدليل من الغلط، أو الخطأ، أو الغش، وهي تكون ضرورية أيضاً لكي تجعل الحقيقة العلمية حقيقة قضائية، فالحقيقة تحتاج دائماً إلى دليل، وإذا كانت هذه الحقيقة قابلة للتطور، فإن الدليل الذي تقوم به الذي قد يصلح أن يتطور لكي يقوى على إثباتها، ويجب ألا يقف هذا التطور عند طرق الحصول على الدليل، بل يلزم أن يتطور أيضاً كل مَن يتعامل مع هذا الدليل من محققين وخبراء وقضاة؛ لأنه بهذا التطور الأخير تتطور الحقيقة القضائية وتستطيع أن تجعل الحقيقة العلمية حقيقة عادلة[1].

---

(1) رستم هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، 1994م.

القسم الثاني

المعاينة في الجريمة المعلوماتية

مع تزايد استخدام الكمبيوتر، والانترنت، والشبكات الداخلية والخارجية تزايدت نسبة الجريمة المرتكبة باستخدام هذه التقنيات الجديدة، وسوف يعمد مرتكبو الجرائم سواء أكانت جريمة تمت عبر الكمبيوتر أم جريمة تمت على الكمبيوتر (بمشتملاتها المادية والمعنوية وقواعد البيانات المستخدمة به)، إلى استخدام الكمبيوتر والشبكة العالمية (الانترنت)، ما داموا يشعرون أن أجهزة إنفاذ القانون، ورجال القضاء، والنيابة، والمحامين، ورجال البحث الجنائي عاجزون عن ضبطهم واستخلاص دليل إدانتهم [1].

وعلى الرغم من أن التعامل في مسرح الجريمة يتطلب إجراءات معينة لحماية الدليل الجنائي الرقمي وإبراز قيمته الاستدلالية إلا أن طرق حفظ الأدلة واستخلاصها تختلف من مسرح الجريمة المادي إلى مسرح الجريمة، ذلك أن التطبيقات أو البرامج والبيانات المرقّمة عنصران أساسيان يتحتم على أجهزة إنفاذ القانون وخبراء الأدلة الجنائية، جمعهما واستخلاصهما. والمعاينة في جوهرها ملاحظة وفحص حسي مباشر بمكان أو شخص له علاقة بالجريمة، وذلك لإثبات حالته والكشف والتحفّظ على ما قد يفيد من الأشياء في كشف الحقيقة قبل أن تنالها يد العبث والتخريب، وهي صورة من صور الحصول على الإيضاحات. والمعاينة من الوجهة القانونية ليست وسيلة إثبات بل هي إجراء استقصائي كاشف لأبعاد الجريمة وأركانها [2].

---

(1) عوض، رمزي رياض، مشروعية الدليل الجنائي في مرحلة المحاكمة وما قبلها، دراسة تحليلية تأصيلية مقارنة، دار النهضة العربية، القاهرة، 1997م.

(2) رستم، هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، المرجع السابق.

المبحث الأوَّل

مفهوم المعاينة وطبيعتها في الجريمة المعلوماتية

المطلب الأوَّل

مفهوم المعاينة

المعاينة هي أهم إجراء من إجراءات التحقيق قاطبة يجوز للنيابة العامة أن تقوم به في غيبة المتهم إذا لم يتيسر حضوره، والمعاينة لها أهمية قصوى في إثبات الواقعة، وسوف نتناولها من عدَّة جوانب لتحديد ماهيتها والسلطة المختصة بإجرائها، وأهميتها القانونية والعملية، والشروط الواجب توافرها لصحتها الاستعانة بأهل الخبرة في إجرائها. والمعاينة هي إثبات الحالة، والمراد بهذا إثبات حالة الأشخاص والأشياء والأمكنة ذات الصلة بالحادث. والمعاينة إجراء من إجراءات التحقيق [1].

والمعاينة في اللغة نظر الشيء ومشاهدته، وفي الاصطلاح الجنائي رؤية محل ارتكاب الوقائع الجنائية وإثبات حالتها بالشكل الذي تركها به الجاني عقب ارتكاب الجريمة، كما تنصرف إلى فحص جسم المجني عليه والمتهم وإثبات ما يوجد بهما من الآثار[2].

والمعاينة هي: «أثبات مادي ومباشر لحالة الأشخاص والأشياء والأمكنة

---

(1) إبراهيم، خالد ممدوح الجرائم المعلوماتية، الدليل الإليكتروني في الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2007م.

(2) يوحويش، عطية عثمان محمد، حجية الدليل الرقمي في إثبات جرائم المعلوماتية، رسالة التخصص العالي (الماجستير)، المرجع السابق.

ذات الصلة بالحادث»، والمعاينة هي: «إجراء بمقتضاه ينتقل المحقّق إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة، وكيفية وقوعها ،وكذلك جمع الأشياء الأخرى التي تفيد في كشف الحقيقة، فالمعاينة في علم التحقيق الجنائي هي مشاهدة المكان الذي ارتُكبت فيه الجريمة وعمل وصف شامل له سواء بالكتابة، أو بالرسم التخطيطي، أو بالتصوير لإثبات حالته بالكيفية التي تركها بها الجاني كما تشمل فحص جسم المجني عليه والمتهم، وبيان ما يوجد بهما من آثار مما يتخلّف عن الجريمة، أو مما له علاقة بها»[1].

والمحرك الأساسي لنقطة الانطلاق والذي بمقتضاه تسارع السلطات المختصة بالانتقال لإجراء المعاينة إما أن يكون الإبلاغ الذي تم من أي فرد، أو الشكوى الصادرة من صاحب الشأن، أو وصول وقوع الجريمة إلى علم مأمور الضبط القضائي بأي طريقة، أو مشاهدة الجريمة في حالة تلبُّس. ورغم أن ظاهر النص يُشير إلى ضرورة الانتقال والمعاينة في حالة التلبُّس بجناية أو جنحة، إلا أنه لا يتصور وجود هذه الضرورة إذا لم يكن للجريمة محل مكاني تنطبع فيه آثار ارتكابها كجرائم التزوير المعنوية، والرشوة، وجريمة السب التي تقع بالقول في غير علانية وغيرهما، لم يكن ثمة مجال أو مقتضي لإجرائها. وحتى تأتي المعاينة بثمارها وتفي بأغراضها المنشودة نجد أن بعض التشريعات الوطنية قد قررت جزاءات جنائية على كل مَن يقوم بإجراء أي تغيير على حالة الأماكن التي وقعت فيها الجريمة، أو ينزع أي شيء منها قبل الإجراءات الأولية للتحقيق القضائي، إلا أن تلك التغييرات أو نزع الأشياء للسلامة والصحة العامة [2].

---

(1) رستم، هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، المرجع السابق.

(2) حسني، محمود نجيب، شرح قانون العقوبات، القسم الخاص، الجرائم المضرة بالمصلحة العامة، دار النهضة العربية، القاهرة 1972م.

المطلب الثاني

طبيعة المعاينة

المعاينة قد تكون إجراء تحقيق أو استدلال الذي يستهدف استظهار الحقيقة في واقعة أو جريمة تبلغ أمرها إلى السلطات، وذلك لكشف عناصرها وأركانها وجمع أدلة الإثبات فيها عن طريق حصر، ومناظرة مكوّنات المكان الثابتة، وموجوداته المنقولة من أجهزة وأدوات وآثار ناشئة عن وقوعها.

ولا تتوقف طبيعتها على صفة مَن يجريها، بل على مدى ما يقتضيه إجراؤها من مساس بحقوق الأفراد، فإذا جرت المعاينة في مكان عام كانت إجراء استدلال، وإذا اقتضت دخول مسكن أو له حرمة خاصة كانت إجراء تحقيق. والمعاينة جوازية للمحقّق شأنها شأن سائر إجراءات التحقيق فهي متروكة إلى تقديره سواء طلبها الخصوم أو لم يطلبوها، ولا تتمتع المعاينة في مجال كشف غموض الجريمة المعلوماتية بنفس الدرجة من الأهمية التي تلعبها في مجال الجريمة التقليدية [1].

وإذا كان محل المعاينة مكان، أو شخص، أو شيء فهو في المجال المكاني مسرح الحادث أو الجريمة كموقع وميدان لها مارس فيه الجاني أو الجناة أنشطتهم الموجهة نحو التنفيذ دون أن تمتد إجراءات المعاينة إلى مستودع الأسرار وإلا دخلت في نطاق إجراء جنائي آخر هو التفتيش بما له من أحكام وقيود ينفرد بها عن المعاينة. أما محل المعاينة بالنسبة للأشياء القائمة والموجودة بالمكان من مكوّنات ثابتة، أو محتويات منقولة، أو آثار، ومخلفات لها صلة بكشف الحقيقة. لهذا يُطلق على عمليات التقصي والتنقيب عن الأشياء والآثار بمسرح الجريمة بمقتضى المعاينة تعبر عن «البحث»، إذ أن الأخير يقتصر في معناه القضائي على مستودع أسرار المتهم أو غير المتهم، سواء

(1) إبراهيم، خالد ممدوح الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2009م.

بداخل جسمه أو بملابسه وأمتعته التي في حوزته أو في مسكنه، ويعتمد هذا الإجراء في تنفيذه على القسر والقهر باعتباره إجراء يُتخذ ضد شخصية معينة بذاتها هي شخصية المتهم أو غير المتهم في الحالات التي يجوز فيها تفتيشه، وذلك وفق قواعد وأصول إجرائية محدودة تنص عليها التشريعات الجنائية ويلتزم بها القائم على التنفيذ وإلا تعرَّض الإجراء للبطلان وذلك صوناً لحرمة المساكن [1].

المطلب الثالث

أهمية المعاينة في الجريمة المعلوماتية

المعاينة عصب التحقيق الجنائي ودعامته وعماده فهي تُعبر عن الوقائع والحقيقة تعبيراً صادقاً لا تكذب ولا تحابي ولا تخدع فتعطي المحقِّق صورة واقعية لمكان الجريمة وما يتصل بها من ماديات وآثار. وللمعاينة أهمية بالغة في أدلة الدعوى وفي إقناع المحكمة في كثير من القضايا، ويبدو هذا في أن ماديات الواقعة يكون من العسير، في الغالب، العبث بها، ونادراً ما تخفي الحقائق، خلافاً لأقوال الشهود الذين قد يتأثرون بدوافع معينة فيكذبون فتضيع الحقيقة نتيجة لذلك، والمعاينة كإجراء من الإجراءات الهامة في مجال التحقيق الجنائي، سواء من الناحية القانونية أو العملية، فهي مرآة صادقة تعكس بأمانة ما فعله الجاني من جرم بلا تجني أو مبالغة فهي ناطقة بما أتاه شاهدة على ما فعله دون شطط أو نقصان، ومن ثم فإنه ليس غريباً أن تكون مجالاً لعلم مستقل لأهميتها، إذ من الناحية القانونية، تبدو الأهمية القانونية للمعاينة في الجرائم المعلوماتية من عدة نواحي منها، تأكيد وقوع الجريمة

---

(1) الطوالبه، علي حسن، مشروعية الدليل الإليكتروني المستمد من التفتيش الجنائي، «دراسة مقارنة الحقوق جامعة العلوم التطبيقية، البحرين، 2005م.

ونفيها، صدق أقوال أطراف الواقعة، ركن الخطأ أو العمد في الواقعة، تحديد الوصف القانوني للواقعة، وتساعد القاضي على تكوين اقتناعه [1].

ومن الناحية العملية تساعد المحقِّق على تحديد وقت ارتكاب الجريمة، ومعرفة علاقة الجاني بالمجني عليه، وتُحدد الأسلوب الإجرامي للجاني، ومع التسليم بأهمية المعاينة في كشف غموض الكثير من الجرائم التقليدية وجدارتها بتبوء مكان الصدارة فيما عدا حالات استثنائية على ما عداها من الإجراءات الاستقصائية الأخرى، إلا أن دورها في مجال كشف غموض الجرائم المعلوماتية وضبط الأشياء التي قد تُفيد في إثبات وقوعها ونسبتها إلى مرتكبها لا ترق إلى نفس الدرجة من الأهمية، وذلك لعدة أسباب منها:

1 - أن الجرائم التي تقع على نظم المعلومات والشبكات قلما يخلف عن ارتكابها آثاراً مادية.

2 - إمكانية التلاعب في البيانات عن بعد، أو محوها عن طريق التدخل من خلال وحدة طرفيه من قِبل الجاني.

3 - أن عدداً كبيراً من الأشخاص قد يتردد على المكان أو مسرح الجريمة خلال الفترة الزمنية الطويلة نسبياً والتي تتوسط عادة بين زمن ارتكاب الجريمة وبين اكتشافها مما يُفسح المجال لحدوث تغير، أو إتلاف، أو عبث بالآثار المادية، أو زوال بعضها وهو ما يُلقي ظلالاً من الشك على الدليل المستمد من المعاينة.

---

(1) بوحويش، عطية عثمان محمد، حجية الدليل الرقمي في إثبات جرائم المعلوماتية، رسالة التخصص العالي (الماجستير)، المرجع السابق.

المبحث الثاني

السلطة المختصة بإجراء المعاينة في الجريمة المعلوماتية

المعاينة كإجراء من إجراءات التحقيق ومن اختصاص سلطات التحقيق، وهذا ما أشارت إليه النصوص القانونية المختلفة، حيث نجد المادة (24) من قانون الإجراءات الجنائية المصري تنص على أن: «مأموري الضبط القضائي يقومون بإجراء المعاينة اللازمة لتسهيل تحقيق الوقائع التي تبلغ إليهم واتخاذ جميع الوسائل التحفيظية اللازمة للمحافظة على أدلة الجريمة».

ونصت المادة (231) إجراءات على وجوب انتقال عضو النيابة بمجرد إخطاره بجناية متلبس بها، وذلك ليثبت حالة الأمكنة والأشياء والأشخاص ووجود الجريمة مادياً، وكل ما يلزم لإثبات حالتها، ويجب الإسراع في الانتقال للمعاينة حتى لا يتطرَّق الشك إلى الدليل المستفاد منها، وذلك إذا ما انقضت فترة ما بين الوقوع وإجراء المعاينة تسمح بأن يتمكن الجاني من إزالة بعض العناصر المادية التي تُفيد في كشف الحقيقة.

مفاد ما سبق، أنه يلزم أن يتولى المعاينة رجل الضبط القضائي أو المُحقِّق، وتنصب مباشرة على المحل والموضوع دون وسيط، فلا يجوز أن تستقي عناصرها ويعول عليها من وسيط ناقل كالشاهد أو المجني عليه [1].

وتتم المعاينة في الجرائم المعلوماتية المرتكَبة عبر الانترنت كأي جريمة أخرى عن طريق الانتقال إلى محل الواقعة الإجرامية، إلا أن الانتقال هنا لا يكون إلى العالم المادي، وإنما إلى العالم الافتراضي أو عالم الفضاء الإليكتروني، فالمعاينة تتم بالانتقال إلى محل الواقعة الإجرامية كقاعدة

---

(1) حسن، سعيد عبد اللطيف، الإثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، الجرائم الواقعة في مجال تكنولوجيا المعلومات، ط1، دار النهضة العربية، القاهرة، 1999م.

إجرائية مقررة في هذا الشأن إلا إنه في إطار جرائم الانترنت، فإن الانتقال يُعد من الموضوعات الجديدة، ذلك أن مسألة الانتقال هذه لا تكون بالضرورة عبر العالم المادي، وإنما يجب أن تكون بالضرورة عبر العالم الافتراضي [1].

وهناك عدة طرق يستطيع بها عضو سلطة التحقيق أو مأمور

الضبط القضائي أن ينتقل إلى عالم الفضاء الإليكتروني لمعاينته، وذلك من خلال:

1 - من خلال مكتبه بالمحكمة من خلال الكمبيوتر الخاص به.

2 - ويمكنه اللجوء إلى مقهى الانترنت.

3 - ويستطيع المحقِّق أيضاً الانتقال إلى العالم الافتراضي للمعاينة من خلال مقر مكتب الخبير التقني المختص إذ توفر له في القانون ما يُبيح ذلك، ولعل هذا متوافر، في مصر، من خلال إدارة مكافحة جرائم المعلوماتية التابعة لوزارة الداخلية.

وذلك أنه في كل الأحوال يلزم أن يقوم عضو التحقيق بالمعاينة من خلال كمبيوتر أو والتشغيل. ثم فإن مشكلة الانتقال المادي إلى محل ارتكاب الوقعة الإجرامية لا تُشكل ذلك العائق أمام عضو التحقيق، وإنما المشكلة تكون من خلال الانتقال إلى العالم الافتراضي حيث يلزم أن يكون هذا الانتقال بالسرعة الكافية التي تمنع زوال آثار الجريمة [2].

ويجب على المحقِّق الجنائي قبل الانتقال لإجراء معاينة لمسرح الجريمة المعلوماتي اتباع ما يلي:

---

(1) الصغير، جميل عبد الباقي، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، الطبعة الأولى، منشورات دار النهضة العربية، القاهرة، 1992م.

(2) الصغير، جميل عبد الباقي، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، (أجهزة الرادار – الحاسبات الآلية – البصمة الوراثية)، دراسة مقارنة، المرجع السابق.

1 - توفير معلومات مسبقة عن مكان الجريمة ومن المالك لهذا المكان، ونوع وعدد أجهزة الكمبيوتر المتوقع مداهمتها وشبكاتها، لتحديد إمكانيات التعامل معها فنياً من حيث الضبط والتأمين وحفظ المعلومات.

2 - الحصول على الاحتياجات الضرورية من الأجهزة والبرامج للاستعانة بها في الفحص والتشغيل.

3 - قطع التيار الكهربائي عن موقع المعاينة لشل فاعلية الجاني في القيام بأي فعل من شأنه التأثير أو محو آثار الجريمة.

4 - إعداد فريق تفتيش من المتخصصين والفنيين.

5 - إعداد الأمر القضائي اللازم للقيام بالتفتيش، سواء كان ذلك أمر من النيابة العامة أم أمر من القاضي الجزئي المختص وذلك في الحالات التي حددها القانون.

سابعاً: شروط صحة معاينة مسرح الجريمة المعلوماتية:

وفور تلقي المحقق البلاغ والتأكد من صحة وقعه عليه أن ينتقل إلى مكانه لذا نجد المادة (296) تعليمات تنص على انه«ينتقل عضو النيابة في الوقت المناسب إلى مكان الحادث ويعاينه...».

وفى سرعة الانتقال المحقق فوائد عظيمة منها، ضمان عدم تغيير شكل مسرح الجريمة عن الوضع والحالة التي تركه الجاني عليها، والحصول على شهود للواقعة، بل قد يكون الجاني موجوداً ومقبوضاً عليه بمسرح الجريمة.

السيطرة على مكان وقوع الجريمة المعلوماتية:

بمجرد وصول المحقق لمكان الحادث لمعاينته أن يقوم بالسيطرة عليه وذلك بإتباع الإجراءات التالية:

1 - حصر الذين تواجدوا بداخل مسرح الجريمة بعد هروب الجاني

واكتشاف الواقعة وتدوين كافة بياناتهم وصلتهم بالواقعة وأطرافها.

2 - منع تواجد أحد بداخل مسرح الجريمة حتى لا يؤثر ذلك على الآثار والأدلة المعثور عليها بقصد أو بخطأ.

3 - التأكد من عدم لمس أية آثار أو أدوات بداخل مسرح الجريمة لذا يفضل على مَن يدخل لمسرح الجريمة بحكم عمله أن يضع يديه بداخل البنطلون الذي يرتديه حتى يطمئن تماماً لعدم لمس أية أشياء.

4 - التحفظ على ما له علاقة بالحادث من أمكنة وأشياء وأشخاص.

5 - إخطار الخبراء لرفع الآثار التي بمكان الحادث كل وفقاً اختصاصه على أننا ننوه في ذلك المجال ونؤكد أن أول خبير يقوم بعمله هو خبير التصوير.

ولضمان تحقيق تلك السيطرة على مسرح الجريمة أن يقوم المحقق بتعيين بعض معاونيه على جميع الجهات الخاصة بالمكان لمنع أحد من التردد عليه.

الفصل السادس

الإثبات أمام المحكمة الرقمية

(الدليل الجنائي الرقمي)

المبحث الأوَّل

مفهوم الدليل الجنائي الرقمي وطبيعته

المطلب الأوَّل

مفهوم الدليل الجنائي الرقمي

الدليل بوجهٍ عام هو أداة الإثبات عموماً، ويُقصد بهذا الإثبات القواعد المتعلِّقة بالبحث عن الأدلة وإقامتها أمام القضاء وتقديرها من جانبه للوصول إلى حكم بشأن الواقعة محل الإثبات. ويقتصر الإثبات على إثبات الوقائع لا بيان وجهة نظر المشرِّع وحقيقة قصده، فالبحث في هذا يتعلق بتطبيق القانون وتفسيره وهو من عمل المحكمة. وينقسم الإثبات إلى نوعين، الإثبات بالأدلة المباشرة والتي هي الاعتراف والشهادة والخبرة والمعاينة لمسرح الواقعة، والإثبات بالأدلة غير المباشرة والتي يصل القاضي إلى الحقيقة منها

عن طريق الاستقراء والاستنتاج. وهذا الإثبات في نوعيه يخضع لمبدأ الإثبات الحر والذي يعتمد على حرية القاضي الجنائي في الاقتناع [1]. وهذا الدليل يمكن تعريفه بوجهٍ عام بأنه: ما تنهض به الحجة لثبوت قضية. وفي القضاء يُقصد به ما يُستعان به في مجلسه لإثبات الواقعة ومدى صحتها لاقتناص يقين القاضي بوجه الحق في الدعوى المعروضة عليه. وغاية الدليل الوصول إلى الحقيقة سواء أثبت وقوع الجريمة وأسندها إلى المتهم بارتكابها أم أثبت عدم إمكان إسنادها إليه. فأهمية الدليل في المواد الجنائية أهمية عظيمة لأنه هو الذي يُناصر الحقيقة ويبين مرتكب الجريمة، وهو الذي يحول الشك إلى يقين. فالحقيقة في معناها العام تعني معرفة حقيقة الشيء بأن يكون أو لا يكون، وهذا لا يتحقَّق إلا بالدليل بحسبان أنه المعبِّر عن هذه الحقيقة. والقضاء في الشريعة الإسلامية الغراء يحتاج إلى بينة لإثبات الحق، وهذا ثابت بحديث رسول الله ﷺ، فعن ابن عباس رضي الله عنهما أن النبي ﷺ قال: «لو يعطي الناس بدعواهم لادعى ناسٍ دماء رجالٍ وأموالهم، ولكن اليمين على المدَّعى عليه، وفي رواية أخرى لبيهقي بإسناد صحيح: «البينة على المدَّعي واليمين على مَن أنكر». ولا يغيب عن الذهن أن البحث عن الدليل يجب أن يتم في إطار الشريعة الإجرائية وفي إطار مبدأ أن الأصل في المتهم البراءة، فالحق في الدليل يجب أن يتركز على حماية كرامة وشرف الإنسان. ولذلك فإن وسائل البحث عن الدليل تسير في ركب مبدأين الأول: الحرية في الوصول إلى الدليل، وأما الثاني: الشرعية في الوصول إلى هذا الدليل [2].

ويمكن تعريف الدليل الإليكتروني بأنه: الدليل الناتج عن استخدام الوسائل الإليكترونية في ارتكاب الأفعال غير المشروعة التي تقع على العمليات الإليكترونية، أو الذي ينتج عن الجرائم التي تقع على الوسائل المعلوماتية،

---

(1) عرب، يونس، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، المرجع السابق.

(2) بوحويش، عطية عثمان محمد، حجية الدليل الرقمي في إثبات جرائم المعلوماتية، رسالة التخصص العالي (الماجستير)، المرجع السابق.

أو الذي ينتج عن الجرائم التي تقع على الوسائل المعلوماتية ذاتها، والذي يتميَّز في الغالب في صوره بالطبيعة الفنية والعلمية تمشيا مع الطبيعة الفنية الخاصة التي تتميَّز بها الجرائم التي يكون معداً لإثباتها.

ويُعرِّف البعض من الفقه الدليل الإليكتروني بأنه: «هو الدليل المأخوذ من أجهزة الكمبيوتر، وهو يكون في شكل مجالات، أو نبضات مغناطيسية، أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، وهي مكوّن رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة، أو الصور، أو الأصوات، والأشكال، والرسوم؛ وذلك من أجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون» [1]. والدليل الإليكتروني يمكن تقسيمه إلى ثلاث مجموعات، وهي كالتالي:

1 - السجلات المحفوظة في الكمبيوتر، وهي الوثائق المكتوبة والمحفوظة مثل البريد الإليكتروني وملفات برامج معالجة الكلمات ورسائل غرف المحادثة على الانترنت.

2 - السجلات التي تم إنشاؤها بواسطة الكمبيوتر، وتعتبر مخرجات برامج الحاسوب وبالتالي لم يلمسها الإنسان مثل log files وسجلات الهاتف وفواتير أجهزة السحب الآلي.

3 - السجلات التي جزء منها تم حفظه بالإدخال، وجزء آخر تم إنشاؤه بواسطة الكمبيوتر، ومن الأمثلة عليها أوراق العمل المالية التي تحتوي على مدخلات تم تلقيمها إلى برامج أوراق العمل مثل Excel ومن ثم تمت معالجتها من خلال البرنامج بإجراء العمليات الحسابية عليها.

وإذا كانت الأدلة المتحصلة عن الوسائل الإليكترونية قد توجُّس منها

---

(1) إبراهيم، خالد ممدوح الجرائم المعلوماتية، الدليل الإليكتروني في الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2007م.

كل من القضاء والفقه خيفة من عدم تعبيرها عن الحقيقة نظراً لما يمكن أن تخضع له طرق الحصول عليها من التعرُّض للتزييف والتحريف والأخطاء المتعددة، فإن ذلك قد تطلب وجوب توافر مجموعة من الشروط التي قد تضفي عليها المصداقية ومن ثم اقترابها نحو الحقيقة وقبولها كأدلة إثبات في المواد الجنائية [1]. وإذا كانت الأدلة التقليدية تقوى بسهولة على إثبات الجرائم عامة، إلا أنها قد لا تقوى على إثبات الجرائم التي تُرتكب بالوسائل الإليكترونية فهذه الوسائل سواء أكانت أداة في ارتكاب الجريمة أم كانت محلاً لها تساعد على إخفاء الآثار التي تترتب عليها، مما يعوق الحصول على الأدلة التي قد تتحصل منها. فنحن نعلم بأن سلطات جمع الاستدلالات والتحقيق قد اعتادت على أن يكون الإثبات مادياً تبصره الأعين وتدركه الحواس وتلمسه الأيدي وأما في محيط الانترنت وغيره من وسائل الاتصال المختلفة فإن المتحري أو المحقق لا يستطيع تطبيق إجراءات الإثبات التقليدية على المعلومات والتي تتميز بطبيعة معنوية. كذلك فإن الجرائم التي تقع على الوسائل الإليكترونية قد تحتاج إلى خبرة فنية متخصصة لكي يمكن البحث عن الأدلة التي تثبتها وذلك من خلال البحث في ذاكرة هذه الوسائل كالأقراص الصلبة وغيرها [2]. أيضاً فإن الوسائل المعلوماتية ذاتها قد تكون الأداة في ارتكاب الجرائم وهي بذلك تكون دليلاً لإثبات هذه الجرائم. وليس بِخافٍ أن هذا الإثبات سيكون محفوفاً بالمخاطر بالنظر إلى وجود خطر أو شبهة التحريف الإداري أو اللاإداري للأدلة التي يتمخَّض عنها هذا الإثبات. ويُلاحظ كذلك أن الطبيعة المعنوية للمحررات الإليكترونية والتي لا يترك التلاعب أو الغش في محتواها أو فيما أُعدت لإثباته آثاراً ملموسة تُشكل صعوبة كبيرة في عملية إثبات جرائم الغش والتزوير التي تقع على هذه المحررات.

---

(1) إبراهيم، خالد ممدوح الجرائم المعلوماتية، الدليل الإليكتروني في الجرائم المعلوماتية، المرجع السابق.

(2) الفيومي، محمد، «مقدمة في علم الحاسابات الإليكترونية والبرمجة بلغة «بيسك»، دار الفرقا، 1984م.

المطلب الثاني

طبيعة الدليل المتحصل من الجرائم المعلوماتية

لقد أثّر التقدم العلمي على الواقع الذي يُطبق عليه القانون، وأثّر كذلك على القانون الذي يُطبق على هذا الواقع. وهذا يترتب عليه - بالطبع - تطوراً في الدليل الذي يربط بينهما لأنه هو أداة تطبيق القاعدة القانونية على واقعة محدَّدة. ولا شك في أن التطور الحالي الذي انعكس أثره على الأدلة يستند إلى الآثار الجديدة التي ترتبت على ثورة الاتصالات عن بعد والتي تمخضت عنها حقيقة علمية جديدة غيرت الكثير من المفاهيم التقليدية للقيم والمصالح التي يحميها المشرِّع الجنائي بنصوص التجريم والعقاب، مما ترتب عليه وجوب توفير الحماية لقيم ومصالح معنوية [1]، والاعتراف بالحجية لمستندات غير مادية تتميز بطبيعة إليكترونية، خاصة بعد أن أصبح الكثير من الجرائم المستحدثة في مجال العمليات الإليكترونية يرتكب باستخدام الوسائل الإليكترونية المتقدمة. فلا مرية أن التطور الحالي لثورة الاتصالات سينعكس أثره على الأدلة المتحصلة من الوسائل الإليكترونية بحيث يجعل الحقيقة التي ستتولد منها تقترب إلى الحقيقة العلمية. وهذا يفرض علينا ونحن نقدر قيمة هذه الأدلة في الإثبات الجنائي أن نحاول تقريب هذه الحقيقة العلمية مع الحقيقة القضائية، بحيث أن الأولى تساعد الثانية في إثبات حقيقة وقائع محددة ومدى نسبتها إلى متهم معين. ولعل مما قد يساعد في تحقيق ذلك أن التطور العلمي الحالي في نظام الوسائل الإليكترونية سواء على مستوى الأجهزة أو البرامج قد أضفى عليها مصداقية في مجال المعالجة الإليكتروني للمعلومات وذلك بفضل استخدام معالجات ميكرفونية معقدة ودوائر ذات قدرة عالية من التكامل يمكن أن تضمن أو توفر للحاسبات الآلية

---

(1) الشوا، محمد سامي، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة 1994م.

هذه المصداقية، كما وأن الجيل الحديث من هذه الوسائل تم تزويده بأنظمة مراقبة متعددة تسمح باكتشاف وتحليل أي خلل أو تلاعب بالنسبة للتشغيل أو في البرامج (1). كذلك فقد لحق التطوير تقنيات ذاكرة بعض أنظمة المعلومات عن طريق استخدام بعض أواسط التسجيل مثل اسطوانة الفيديو والكارت ذو الذاكرة، وهذا يضمن تسجيلات على درجة كبيرة من الدقة، فضلاً عن أن هذه التقنية لا تقبل المحو أو التعديل ويمكن لها تسجيل كل عملية تتم من خلالها بما قد يؤدي إلى توافر الدليل عند المنازعة في ذلك. وتجدر الإشارة إلى أن تأثير التطور العلمي لا يقف عند مضمون الدليل وإنما يمتد هذا التأثير كذلك إلى الإجراءات التي يترتب عليها الحصول على هذا الدليل، ولذلك فإنه يجب أن تكون هذه الإجراءات المتطورة ذات طبيعة مشروعة لكي تحافظ على شرعية الأدلة المتولدة منها. وكتطبيق لذلك نجد أن محكمة النقض الفرنسية قد قبلت شرعية الدليل الذي نتج عن إجراء شرعيته. شركة تجارية تُمثل في وضعها لجهاز فيديو مزود بكاميرا خفية في إحدى فتحات التهوية لكي لا يراها أحد وذلك لاكتشاف الأفعال غير المشروعة التي ترتكب بداخلها من المستخدمين بها. ولم تعتبر محكمة النقض أن هذا الإجراء فيه مساس بالحياة الخاصة وبالتالي فلم تهدر شرعيته. ولقد تطلب قضاء هذه المحكمة فيما يتصل بالمراقبة التليفونية بالوسائل العلمية المستحدثة بأن ذلك يتم وفقاً للإجراءات التي نص عليها القانون والتي تُحدد الطرق المشروعة للحصول على الدليل بما يضمن ابتعاد هذه الطرق عن المكر والخداع. وهكذا نرى أن التطور العلمي الذي لحق بالوسائل الإليكترونية قد أثّر تأثيراً كبيراً على الأدلة المتحصلة منها وعلى إجراءات الحصول عليها، فهذا التطور قد جعل أكثر هذه الأدلة يتميز بطبيعة غير مرئية بحيث يصعب الوصول إليها لأنها تكون نتاج تلاعب في رموز ونبضات وإليكترونيات، كما أنه قد زاد من صعوبة إجراءات الحصول عليها لأنه قد أمد الجناة بوسائل متطورة

---

(1) مغايرة، منصور دراسة، حول «الجرائم المعلوماتية»، مكتبة جامعة الحكمة، 1999م – 2000م.

تمكنهم من إخفاء أفعالهم غير المشروعة كاستخدام كلمات السر والتشفير واستطلاعه التلاعب في البيانات المخزّنة، بل وإتلافها في الوقت الذي يرونه مناسباً وفي ثوان معدودة. وعلى ضوء ذلك يمكن القول بأن الدليل المتحصل من الوسائل المعلوماتية يستمد طبيعته من ذات العمليات الإليكترونية التي نتج منها في حالة الاعتداء عليها بالأفعال غير المشروعة. ولذلك فهو يتخذ أيضا طبيعة إليكترونية بحيث قد يصعب عليه إلا باتباع إجراءات معينة يكون الغالب منها ذو طبيعة فنية [1]. وليس أدل على ذلك من أن التلاعب في المستندات الإليكترونية لا يمكن كشفه بالطُرق التقليدية وإنما قد يحتاج ذلك إلى أدلة إليكترونية قد تتحصل من الوسائل المعلوماتية ذاتها أو باستخدام التقنية العلمية المتقدمة التي يتعين اتباعها للوصول إليه. كذلك فإن تقليد التوقيع الإليكتروني أو تزويره لا يمكن كشفه وفقاً للطرق التقليدية المتبعة في ذلك بفحص الخطوط وغيرها، وإنما يلزم لذلك فك رموز وتشفيرات معينة لا يمكن الوصول إليها إلا باستخدام الوسائل الإليكترونية ذاتها. أيضاً فإن هناك أدلة إليكترونية قد ساعد في الحصول عليها استخدام الوسائل الإليكترونية مثال ذلك: استخدام أجهزة الرادار وكاميرات التصوير، وكاميرات الفيديو والسينومتر، والوسائل الحديثة في التصنت، والتسجيلات بمساعدة مسجلات الصوت والتي تستخدم في ضبط الكثير من الجرائم. وتجدر الإشارة إلى أن الأدلة المتحصلة من الوسائل الإليكترونية قد تنتمي إلى أدلة الإثبات التقليدية وذلك إذا كانت نتاج شهادة أو اعتراف أو خبرة، فقد يمكن إثبات جرائم الاحتيال والسرقة والاختلاس في الجرائم الإليكترونية عن طريق الوثائق الأصلية المحفوظة بالميكروفيش، أو بالشرائط الممغنطة، أو بحافظات الأكواد، أو بمخرجات الحاسب، وسجلات التشغيل كما لا يغيب عن الذهن أن الطبيعة الخاصة بالأدلة الإليكترونية ستنعكس – بالطبع – على الطرق التي من خلالها يتم الوصول إليها، بحيث أن الطرق التقليدية المتبعة في البحث

---

(1) عرب، يونس، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، المرجع السابق.

عن الأدلة والوصول إليها لم تعد تصلح أو تكفي للوصول إلى الأدلة المتحصلة من الوسائل الإليكترونية، بل يلزم اتباع طرق جديدة تتناسب مع هذه الأدلة ويمكن باتباعها إثبات الجرائم التي تقع على العمليات الإليكترونية، وهذا ما سنفصله بالبيان، فيما يلي:

1 - الطرق الحديثة للوصول إلى الدليل الإليكتروني وتأثيرها على قوته في الإثبات الجنائي:

من المعروف أن لكل عصر سماته وخصائصه، وسمات العصر الحالي الدخول في عالم ثورة الاتصالات عن بعد وما ترتب عليه من تغيير في نمط الحياة سواء كان ذلك على مستوى الأفراد أو الحكومات، فلقد أصبح التعامل اليوم يتم عن طريق الإليكترونيات التي لا تعتمد على الأشياء المادية المحسوسة وإنما تعتمد على النبضات والذبذبات والتشفيرات، فحلت النقود الإليكترونية محل النقود الورقية، وحلت الشيكات ووسائل الدفع الأخرى الإليكترونية محل الشيكات ووسائل الدفع الورقية، وحلت بطاقات الوفاء وبطاقات الائتمان الإليكترونية مكان الدفع اليدوي وحلت البنوك الإليكترونية محل البنوك التقليدية، وأفل نجم الأوراق التقليدية وأرشيفها ومستنداتها وبزغ بدلاً منها نجم الحاسبات الآلية وما تتمتع به من مدخلات ومخرجات تتمتع بقدرات هائلة، وظهرت كذلك الحكومة الإليكترونية لكي تتعامل عن طريقها أجهزة الحكومة مع بعضها البعض، أو تتعامل الحكومة عن طريقها مع الأفراد. ولا مشاحة أن الأفعال غير المشروعة التي تترتب على مظاهر هذا التطور على النحو سالف الإشارة إليه لا بد أن تتصف بذات صفاته وتتخذ ذات طبيعته، ولذلك فلم تعد الجرائم التي ترتكب بالوسائل الإليكترونية والتي تقع على الصور المختلفة للعمليات الإليكترونية من نوع الجرائم التقليدية، وإنما قد أطلق الفقه عليها الجرائم المعلوماتية أو الجرائم الإليكترونية [1]. ولا شك في أن كشف ستر هذا النوع من الجرائم الذي يرتكب بالوسائل المعلوماتية يحتاج أيضاً إلى طرق إليكترونية تتناسب مع طبيعته

---

(1) خميس، فوزي، جرائم المعلوماتية وحماية الملكية المعلوماتية وبنوك وقواعد المعلومات، محاضرة ألقيت في نقابة المحامين في بيروت بتاريخ 1999/2/25م.

بحيث يمكنها فك رموزه وترجمة نبضاته وذبذباته إلى كلمات وبيانات محسوسة ومقروءة تصلح لأن تكون أدلة إثبات لهذه الجرائم ذات الطبيعة الفنية والعلمية الخاصة. فتطوير الإثبات الجنائي بتطوير طرقه أمر في غاية الأهمية لمواجهة هذا النوع الجديد من الجرائم، لكي نمنع ما يمكن أن يقال من أن صعوبة هذا الإثبات قد يؤدي إلى عدم التجريم. فإذا كانت الوسائل التقليدية قد تكفي لإثبات الجرائم التقليدية، إلا أنها قد تعجز عن إثبات الجرائم التي ترتكب بالوسائل المعلوماتية. فالدليل أثر يولد أو حقيقة تنبعث من الجريمة المرتكبة، ويجب لمنطقية هذا الدليل ومصداقيته أن تكون ولادة طبيعية بحيث أن الحقيقة التي يُعبر عنها تصل إلى القاضي من تلقاء ذاتها ولا يتعجل هذا الأخير الوصول إليها، لأنه إن فعل ذلك قبل أن تصل هذه الحقيقة إليه فإن ولادة الدليل تصبح نتيجة لذلك ولادة قيصرية تكون قد عجلت بميلاده قبل أن يكتمل نموه، ومن ثم فإن الحقيقة التي تنبعث منه – وهذا حاله – تكون زائفة وغير معبرة عن واقع الدعوى. ولذلك فإن طبيعة الدليل تتشكّل من طبيعة الجريمة التي يولد منها، فدليل التزوير مثلا يأتي من إثبات تغيير الحقيقة في المحررات التي يقع عليها، ودليل جريمة القتل العمد قد يولد من فحص الأداة التي استخدمت في القتل وطلقات الذخيرة التي استعملت فيها، ويمكن تطبيق ذلك أيضاً على أدلة إثبات الجرائم المعلوماتية [1] فإثبات جريمة الغش الإليكتروني أو التزوير في المحررات الإليكترونية أو التلاعب في الجانب المعنوي للحاسبات الآلية، يمكن أن يثبت بأدلة إليكترونية تكون ناتجة أيضاً عن الوسائل الإليكترونية. وإذا كان هناك بعض الأدلة التقليدية التي قد تصلح لإثبات الجرائم التي تقع باستخدام الوسائل المعلوماتية، إلا أنها تكون في حاجة إلى تطوير مستمر لكي يمكنها أن تتناسب مع الطبيعة الخاصة بهذه الجرائم. فالخبرة وعلى الرغم من أنها وسيلة إثبات من الوسائل التقليدية إلا أنها تصلح أيضا لإثبات الجرائم التي ترتكب بالوسائل الإليكترونية، ولكنها تتطلب لكي تقوى على ذلك أن يكون الخبير متمتعاً بمستوى عال من العلم والمهارة الفنية التي تُمكنه من أن يشق

---

(1) عرب، يونس، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، المرجع السابق.

طريقه بنجاح في مجال الجرائم التي ترتكب بالوسائل المعلوماتية والتي تقع على العمليات الإليكترونية المختلفة. كذلك فإن التفتيش يمكن أن تتطور طرقه بحيث لا تقف - فقط - عند ضبط الأدوات المادية المستخدمة في ارتكاب الجريمة أو ضبط جسم الجريمة الذي يُحقق نموذجها القانوني، وإنما يمكن لهذه الطرق كذلك أن تتعامل مع الجرائم التي ترتكب بالوسائل المعلوماتية، أو التي تقع على هذه الوسائل، فيمكن تبعاً لذلك تسجيل البيانات المعالجة إليكترونياً بعد تحويلها من النبضات أو الذبذبات أو الإشارات أو الموجات الكهرومغناطيسية إلى أشياء محسوسة تسجل وتخزن على وسائل معينة، وعلى هذه الوسائل يرد التفتيش أو الضبط. أيضاً فإنه ليس بخافٍ علينا أن الطبيعة الفنية للكثير من الأدلة التي تتحصل من الوسائل المعلوماتية قد يجعلها محلاً لفحص معملي يقوم به خبراء، وهؤلاء الخبراء قد يتأثرون في عملهم بآراء شخصية لهم أو نتائج علمية قد تكون غير صحيحة، وهذا قد يترتب عليه تشويشاً في الحقيقة التي يجب أن تتمتع بها هذه الأدلة، مما قد يضلل الاقتناع الذاتي للقضاة عندما ينظرون تقارير الخبرة. فالحقيقة العلمية أو التكنولوجيا الزائفة يمكن أن تزيف الحقيقة التي تثبت من الأدلة الأخرى القائمة في الدعوى التي ينظرها القاضي وذلك إذا أثّرت في اقتناعه ولم يفطن إلى زيفها، فتكون النتيجة المترتبة عليك فساد الحكم الذي سينتهي إليه. ومما قد يؤثر في صحة الدليل المتحصل من الوسائل الإليكترونية أيضاً الإجراءات التي تتبع لأجل الوصول إليه، فإذا كانت هذه الإجراءات وليدة طرق غير مشروعة فإنه سيترتب عليها عدم شرعيتها ومن ثم بطلان الدليل المتحصل منها [1].

والإذن بتفتيش الحاسب الآلي لضبط جرائم تكون محلها الدعامات الإليكترونية للمعلومات المحفوظة به لا بد أن يصدر وفق إجراءات معينة، فإن لم تراع هذه الإجراءات فإن الأدلة المتحصلة منها ستكون تبعاً لذلك غير مشروعة. فالمشرِّع وإن كان يحمي القيم والمصالح بنصوص التجريم والعقاب، فإنه في الوقت ذاته يحمي حريات الأفراد بالنصوص الإجرائية، ولذلك

(1) بلال، أحمد عوض، قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة، دار النهضة العربية، القاهرة، 1994م.

فإن الإجراءات الأولية التي تتبع لضبط الجرائم قد تكون غير مشروعة إذا أهدرت هذه النصوص الإجرائية؛ لأنها تكون قد خالفت القيم التي يحميها النظام القانوني بهذه النصوص الإجرائية. ولا يغيب عن الذهن أن الجرائم التي تقع على الوسائل الإليكترونية قد تُرتكب كذلك بسبب اختراق الجناة للأمن الإليكتروني للأنظمة والمعطيات الإليكترونية وتمكنهم عن طريق ذلك من الوصول إلى كلمات السر المدخَلة على هذه الأنظمة وارتكاب العديد من الجرائم عليها أو إدخال الفيروسات الضارة إليها. فالجناة الذين يرتكبون هذه الجرائم قد يستطيعون الوصول إلى البصمة الإليكترونية التي تُستخدم في تأمين المستندات وفي تأمين التوقيعات الإليكترونية، وبذلك يمكنهم التلاعب في هذه المستندات وارتكاب العديد من الجرائم عليها. أيضاً فهؤلاء الجناة قد يتمكنون من الوصول إلى مفتاح الشفرة لأنظمة الحاسبات الآلية سواء أكان هذا المفتاح سرياً متماثلاً أم كان خاصاً غير متماثل، وبذلك يستطيعون التلاعب في الجانب المعنوي للحاسب الآلي وفي الشبكات الأخرى التي تربطه بالوسائل الإليكترونية الأخرى. ولا شك في أن الوصول إلى الجرائم التي تُرتكب عن طريق اختراق الأمن الإليكتروني، يتطلب اتباع طرق علمية معينة بحيث يمكن اكتشاف مثل هذا الاختراق وجمع الأدلة التي تثبت وقوعه [1].

وكتطبيق لذلك نجد أنه قد صدر في فرنسا القانون رقم 91 – 646 بتاريخ 10 يوليو 1991م لأجل حماية سرية الاتصالات التليفونية، فوفقاً لهذا القانون لا يمكن الاعتداء على السرية إلا عن طريق السلطة العامة وحماية لمصلحة عامة وباتباع الإجراءات المثبتة في القانون وفي نطاق الحدود التي تنص عليها [2].

---

(1) البشري، محمد الأمين، الأدلة الجنائية الرقمية، مفهومها ودورها في الإثبات، المجلة العربية للدراسات الأمنية والتدريب، المجلد 17، العدد 33، السنة 17، الرياض، أبريل 2002م.

(2) إبراهيم، خالد ممدوح الجرائم المعلوماتية، الدليل الإليكتروني في الجرائم المعلوماتية، المرجع السابق.

المبحث الثاني

صور الدليل الإليكتروني

لا شك في أن الدليل سيظل خاضعاً للتطور بتطور وسائل الحصول عليه، فكلما تطورت هذه الوسائل تطور هو أيضاً، ولذلك نرى أن التطور الذي لحق البحث العلمي قد انعكس أثره على الدليل، فبدأنا نسمع عن دليل البصمة الوراثية وأثره في التعرف على الجناة والذي يتم الحصول عليه عن طريق تحليل الحامض النووي DNA كذلك فإن العلم قد اعتد حديثاً ببصمة قزحية العين، وهي الجزء الموجود خلف العين ومنه تستمد لونها، واعتد أيضاً ببصمة الصوت والشفاه واستخدام هذه البصمات كمفاتيح سر تستخدمه الحاسبات الآلية. وليس هذا إلا قليلاً من كثير ما زال أمره سراً عند علام الغيوب، فصدق قول الله سبحانه وتعالى في قرآنه المجيد: ﴿سنريهم آياتنا في الآفاق وفي أنفسهم حتى يتبين لهم أنه الحق أو لم يكف بربك أنه على كل شيء شهيد﴾ [1]، وقوله سبحانه وتعالى: ﴿ويخلق ما لا تعلمون﴾ [2]. فكلما أفاء الله بخيره على البشرية كشف لهم جزءاً من نعمته فإن أحسنوا استخدامها زادهم من عطائه، وإن أساؤوا استخدامها قتر عليهم بمزيد عطائه بعد أن جحدوا نعمه واضروا أنفسهم بأنفسهم وهم لا يشعرون. ومما أفاء الله به على البشرية ثورة الاتصالات عن بعد والتي لو أنها أحسنت استخدامها فستؤدي لها خدمات عظيمة في تسيير دفة الحياة على مستوى الأفراد ومستوى الحكومات، ولكن الإنسان المستفيد من هذه الثورة بحكم طبيعته البشرية وما يحمله من نفس أمارة بالسوء قد يستخدم هذا التقدم العلمي الجديد في ارتكاب جرائم وبأساليب متطورة مما يلحق الضرر بنفسه، وبغيره وبالمجتمع الذي يعيش فيه. ولذلك نجد أن ثورة الاتصالات عن بعد قد أفرزت

---

(1) سورة فصلت الآية 53.

(2) سورة النحل الآية 16.

جرائم جديدة ذات طبيعة خاصة، وذلك بسبب الطبيعة الخاصة بالوسائل التي تُرتكب بها هذه الجرائم، وبسبب أيضاً الطبيعة الخاصة للقيم والمصالح التي تقع عليها هذه الجرائم، والتي تغير مضمونها بفضل التقدم العلمي فبدأنا نسمع عن البيانات المعالجة آليا والمستندات الإليكترونية والتوقيعات الإليكترونية، والنقود الإليكترونية، وبطاقات الصرف الإليكترونية، والإدارة الإليكترونية [1].

وإن كانت الجرائم التي تقع بالوسائل الإليكترونية أو التي تقع على هذه الوسائل، قد تطورت من حيث طرق ارتكابها ومن حيث الاستفادة من التقنية العلمية في هذا التطور، فإن الدليل المتحصل منها التي قد تصلح أن يتطور بتطورها وذلك لكي يقوى على إثباتها، لأنه إن ظل تقليدياً ومتخلفاً فلن يقوى على هذا الإثبات، وسيترتب على هذا الأمر بالطبع تخلف قانون الإجراءات الجنائية وعدم تطور نصوصه بتطور النصوص الموضوعية للعقاب مما يلحق أشد الضرر بالمجتمع، والأفراد، وبالعدالة.

ولتقدم العلوم المختلفة أثره على توعية الجريمة واستغل المجرم ثمرات في تطوير المخترعات العلمية الحديثة لخدمة اهدافه الإجرامية فبناء دولة إليكترونية حقيقة ثم تحويل العالم إلى قرية كونية في فترة لاحقة ينطوي على ما هو أكبر بكثير من مجرد مد المرافق الأساسية والأسلاك اللازمة فالمشكلة الرئيسية لا تكمن في استغلال المجرمين للانترنت وإنما عجز أجهزة العدالة عن ملاحقتهم وعدم ملاحقة القانون لهم ومسايرته التكنولوجيا الجديدة بتشريعاته أنها حقاً مشكلة التكيف مع العصر ومتغيراته فهذه الهوة، أو التخلف، أو الفراغ التشريعي تبدأ في الظهور نتيجة عدم التجاوب القانوني مع الاحتياجات التي تولدها متغيرات العصر مما يستدعي تغير القوانين لتواكب متغيرات العصر بما يتلاءم مع ما استجد في الحياة من تقنيات

(1) عرب، يونس، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، المرجع السابق.

حديثة ونمط حياة وسلوكيات بشر تختلف اختلافاً جذرياً وجوهرياً عن تلك السلوكيات التي عاصرت عن القوانين المعمول بها[1].

فالعالم قبل ظهور جرائم الانترنت وقبل ظهور الانترنت وجرائمه كانت توجد الأفعال الإجرامية وكانت هذه الأفعال تشمل القتل والسرقة والنصب والتزوير وغيرها من الجرائم فالشر قائم، بيد أن الانترنت ساعد على سهولة ارتكاب هذه الجرائم فتقنيات الكمبيوتر سهلت ارتكاب هذه الجرائم فإذا كانت جرائم الحاسب الآلي تتصف بمستعملين مصرَّح لهم بالتعامل مع برامج الحاسب الآلي كسرقة نقود من بنك ائتمان مثلاً أما جرائم الانترنت فلا يوجد اتفاق عام فيها حول آداب مشاركة كلمة السر ومن الصعب في أغلب الأوقات تحديد هل مستعمل الانترنت أو نظامه مصرَّح له بذلك أم لا وعند الإجابة بنعم أو لا، ففضاء المعلومات ليس له مبادئ الأخلاق عامة فحدود السلوك المقبول أو حتى السلوك الأخلاقي في فضاء المعلومات ليست واضحة فضيف الكمبيوتر يمكنه أولا الوصول إلى بعض المعلومات وعدم الوصول إلى البعض الآخر بينما في الانترنت يمكن الوصول وقراءة البريد الإليكتروني للشخص في الانترنت بسهولة مما يستدعي الأمر تدخل القانون الجنائي[2].

وفي الغالب أن مرتكبي هذه الجرائم من الأفراد ذو المهارات الفنية والتقنية العالية والموظفين ذو الياقات البيضاء والمحتالين وإرهابي التحكم الاتوماتيكي والمبتزين والجواسيس كما أوضحنا فيما سبق، فالانترنت جريمة الأذكياء وحرب المعلومات، فأحد مشاكل الانترنت أن المستعمل يكون مجهولاً وغالباً ما يستخدم أسماء مستعارة بدلاً من اسمه الحقيقي فعدم تحديد الشخصية يشجع ويغري الشخص على ارتكاب جرائم ما كان يفكر فيها فلا

---

(1) قشقوش، هدى، جرائم الحاسب الالكتروني في التشريع المقارن، المرجع السابق.

(2) الصغير، جميل عبد الباقي، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، الطبعة الأولى، منشورات دار النهضة العربية، القاهرة، 1992م.

توجد مبادئ أخلاقية للسلوك المقبول أو المفروض في عالم الانترنت فنزيل الفندق مثلاً يعلم أنه يمكنه الدخول في غرفته طالما يقوم بدفع الحساب ولا يقوم بأي أفعال مزعجة، ويعلم كذلك أنه من حقه استعمال مناطق الفندق العامة مثل البهو والبار والمطعم، ويعلم المناطق الأخرى الخاصة بالفندق مثل المكاتب الإدارية وأماكن التخزين والمطابخ وما أشبه محظورة عموماً، والنزيل يعلم هذه الأشياء دون أن يُحدد له إحداها وتأتي هذه المعرفة من التجربة بيد أنه ليس لفضاء المعلومات تجربة أخلاقية عامة، فحدود السلوك المقبول أو حتى السلوك الأخلاقي في فضاء المعلومات ليست واضحة بعد فلم يواكب التقدم العلمي تقدم خلقي وثمة جرائم يتم ارتكابها من خلال الانترنت مثل النصب والاحتيال، الحصول على المعلومات في حالة نقلها بوسائل تدليسية عبر شبكة الانترنت، واختلاس الأموال [1].

وإن كان يُمثِّل الانترنت رحلة بلا نهاية ولا حدود في عالم المعلومات فالتطورات العلمية الحديثة ترتبط ارتباطاً وثيقاً بأنظمة المعلومات والاتصالات وتعتمد المعلوماتية في انتشارها على أنظمة المعلومات فكلما تقدمت هذه الأنظمة وارتقت كلما أُتيح للمجتمع أن ينمو ويتطور ويتقدم؛ لذلك أصبحت برامج المعلومات تُعد قيمة غير تقليدية نظراً لاستخداماتها المتعددة في كافة المجالات الاجتماعية والاقتصادية. لذلك تبدو أهمية الانترنت بصفته مصدر للمعلومات بالنسبة لأجهزة الكمبيوتر بمثابة القلب من جسم الإنسان فهي لها قيمتها السياسية والاقتصادية والثقافية تلك القيمة جديرة برفعها إلى مصاف الأموال، فيتحدد سعرها بوصفها سلعة قابلة للتداول خاضعة لظروف العرض والطلب، وتُباع وتُشترى في سوق يدور فيه الصراع حول مبالغ هائلة مما أدى إلى ظهور قيمة اقتصادية جديدة وأموال جديدة عرفت بالأموال

---

(1) عرب، يونس، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، المرجع السابق.

المعلوماتية وصاحب ظهور هذا المال المعلوماتي جرائم جديدة عرفت بالجرائم المعلوماتية، وهذه الجرائم يمكن تصورها من زاويتين الأولى تكون المعلوماتية أداة أو وسيلة للغش أو الاعتداء، والزاوية الثانية تكون المعلوماتية موضوعاً للاعتداء، فالاتجاه الاول يستخدم الجاني المعلوماتية لتنفيذ جرائم سواء تعلق منها بجرائم الاعتداء على الأشخاص أو الأموال كالنصب والسرقة وخيانة الأمانة، أما الجرائم من الزاوية يكون المال المعلوماتي محلاً وموضوعاً لها[1].

(1) الصغير، جميل عبد الباقي، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، المرجع السابق.

المبحث الثالث

دور الدليل الجنائي الرقمي في الإثبات

الإثبات الجنائي نشاط إجرائي موجَّه مباشرةً للوصول إلى اليقين القضائي طبقاً لمعيار الحقيقة الواقعية، وذلك بشأن الاتهام أو أي تأكيد أو نفي آخر يتوقف عليه إجراء قضائي، وبمعنى آخر هو إقامة الدليل على وقوع الجريمة ونسبتها إلى فاعل معين[1].

والدليل الرقمي الذي يُعد الوسيلة لإثبات الجرائم التي تُرتكب بالوسائل المعلوماتية أو التي تقع على هذه الوسائل، هو نتاج عمليات فنية وعلمية يكون الجناة قد سلكوها لأجل ارتكاب هذه الجرائم [2]. فالجرائم التي تُرتكب بالوسائل الإليكترونية في صورها الغالبة قد تقع بسبب الغش، أو التزوير، أو التحريف في البيانات المعالجة آلياً عن طريق الحاسبات الآلية، سواء تمت هذه الأفعال أثناء إدخال هذه البيانات، أو أثناء تخزينها، أو أثناء إخراجها. ولذلك فإن الوصول إلى هذه الأفعال يحتاج إلى أدلة علمية وفنية يمكنها أن تثبت وقوعها وتسندها إلى المتهمين بارتكابها [3].

والدليل الرقمي يُعد دليلاً متطوراً؛ لأنه نتاج وسائل إليكترونية متطورة وهو قابل للتطور في المستقبل على ضوء تطور هذه الوسائل، وهو كما سبق القول يمكن إعاقة الوصول إليه بالوسائل الفنية المستحدثة، كما وأن طبيعته

---

(1) مصطفى، محمود محمود، شرح قانون الإجراءات الجنائية، ط11، القاهرة، 1976م.

(2) عثمان، آمال عبد الرحيم، الإثبات الجنائي ووسائل التحقيق العلمية، دار النهضة العربية، القاهرة، 1975م.

(3) إبراهيم، خالد ممدوح الجرائم المعلوماتية، الدليل الإليكتروني في الجرائم المعلوماتية، المرجع السابق.

غير المرئية قد تُعيق إثباته للجرائم التي يكون مُعد لإثباتها [1].

فالأدلة الرقمية ستزداد أهميتها في الوقت الحالي، وذلك بعد أن اعترفت الكثير من التشريعات بالمحررات الإليكترونية ومنحها حجيتها في الإثبات. واعترف أيضاً بالتوقيع الإليكتروني في مجال البيانات المعالجة آلياً عن طريق الحاسبات الآلية وشبكات الانترنت، وأجاز كذلك التعامل ببطاقات الصرف الآلية. ومد حمايته الجنائية إلى الجانب المعنوي الذي تتكون منه الحاسبات الآلية معترفاً بصلاحيته لأن يكون محلاً لارتكاب العديد من الجرائم عليه كجرائم السرقة، والنصب، وخيانة الأمانة، والغش، والإتلاف [2].

والهدف من الإثبات هو بيان مدى التطابق بين النموذج القانوني للجريمة وبين الواقعة المعروضة، فإنه في سبيل ذلك يستخدم وسائل معينة هي وسائل الإثبات، ووسيلة الإثبات هي كل ما يستخدم في إثبات الحقيقة – فهي نشاط يُبذل في سبيل اكتشاف حالة، أو مسألة، أو شخص، أو شيء ما، أو ما يفيد في إظهار عناصر الإثبات المختلفة – أي الأدلة – ونقلها إلى المجال الواقعي الملموس[3]، وتُثير مسألة الإثبات في نظم الحاسوب والانترنت صعوبات كبيرة أمام القائمين على التحقيق، وذلك لجملة أمور لا يسعنا ذكرها كلها[4]، لكن نذكر أمثلة منها: كالتخزين الإليكتروني للمعطيات الذي يجعلها غير مرئية وغير مفهومة بالعين المجردة، ويُشكل انعدام الدليل المرئي (المفهوم) عقبة

---

(1) حجازي، عبد الفتاح بيومي، الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت، دار الكتب القانونية، القاهرة 2002م.

(2) إبراهيم، خالد ممدوح الجرائم المعلوماتية، الدليل الإليكتروني في الجرائم المعلوماتية، المرجع السابق.

(3) عثمان، آمال عبد الرحيم، الإثبات الجنائي ووسائل التحقيق العلمية.

(4) حسن، سعيد عبد اللطيف، الإثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، الجرائم الواقعة في مجال تكنولوجيا المعلومات، ط1، دار النهضة العربية، القاهرة، 1999م.

كبيرة أمام كشف الجرائم، وقد يُشكل تشفير البيانات المخزنة إلكترونياً، أو المنقولة عبر شبكات الاتصال عن بُعد عقبة كبيرة أمام إثبات الجريمة المعلوماتية والبحث عن الأدلة، كما أن سهولة محو الدليل في زمن قصير تُعد من أهم الصعوبات التي تعترض العملية الإثباتية في مجال جرائم الحاسب والانترنت، ومن الأمثلة الواقعية على ما تقدم ما حصل في دولة الإمارات العربية المتحدة، حيث قام مشغّل حاسوب بتهديد المؤسسة التي يعمل لديها بتنفيذ مجموعة من مطالبه، وذلك بعد أن حذف كافة البيانات الموجودة على الجهاز الرئيسي للمؤسسة، وقد رفضت المؤسسة الاستجابة لمطالبه فأقدم على الانتحار، ووجدت المؤسسة صعوبة في استرجاع البيانات التي كانت قد حُذفت[1]، وتتعقد المشكلة عندما يتعلّق الأمر بمعلومات أو بيانات تم تخزينها في الخارج بواسطة شبكة الاتصال عن بُعد، والقواعد التقليدية في الإثبات لا تكفي لضبط مثل هذه المعلومات بحثاً عن الأدلة وتحقيقها، فمن الصعب إجراء التفتيش للحصول على الأدلة في هذه الحالة في داخل دولة أجنبية، حيث أن هذا الإجراء يتعارض مع سيادة هذه الدولة الأخيرة، ولما كانت أدلة الإثبات المتحصلة من التفتيش على نظم الحاسب والانترنت تحتاج إلى خبرة فنية ودراية فائقة في هذا المجال[2]، فإن نقص خبرة سلطات جمع الاستدلالات والتحقيق والمحاكمة قد يؤدي إلى ضياع الدليل بل تدميره أحياناً[3]، ويُضاف إلى ذلك أن كل المعطيات ليس لها تجسيد دائم على أية دعامة، بمعنى أنها لا توجد مسجّلة على أسطوانة صلبة أو مرنة ولا على أية

---

(1) رستم، هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، 1994م.

(2) الكركي، كمال، جرائم الحاسوب ودور مديرية-الأمن في مكافحتها، ورقة عمل مقدمة إلى ندوة قانون حماية حق المؤلف، نظرة إلى المستقبل، المنعقدة في عمان بتاريخ 1999/7/5م.

(3) أسامة أحمد المناعسة وجلال محمد الزعبي وصايل الهواوشة، جرائم الحاسب الآلي والإنترنت، دراسة تحليلية مقارنة، ط1، دار وائل، عمان، 2001م، ص 289-297.

دعامة مادية منقولة أيًا كانت فقد توجد هذه المعطيات في الذاكرة الحية للحاسب، ويتم محوها في حالة عدم حفظها أو تسجيلها على أية أسطوانة، وحتى لو كانت المعطيات قد تم تخزينها على دعامة مادية إلا أنه قد يكون من الصعب الدخول إليها بسبب وجود نظام معلوماتي للحماية، وعلاوة على ذلك قد يتقاعس المجني عليه عن التبليغ عن الجرائم المعلوماتية إلى السلطات المختصة[1]، بالإضافة لما تقدم من صعوبات ومشكلات[2].

(1) الصغير، جميل عبد الباقي، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، (أجهزة الرادار – الحاسبات الآلية – البصمة الوراثية)، دراسة مقارنة، دار النهضة العربية، القاهرة، 2001م.

(2) شتا، محمد محمد، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، 2001م.

المبحث الرابع

دور الدليل الجنائي الرقمي المستمَد من التفتيش

إن الأدلة الرقمية، إما أن تكون مخرجات ورقية يتم إنتاجها عن طريق الطابعات، أو الراسم، وإما أن تكون مخرجات غير ورقية أو أن تكون إليكترونية: كالأشرطة والأقراص الممغنطة وأسطوانات الفيديو وغيرها من الأشكال الإليكترونية غير التقليدية[1]، أو تتمثّل في عرض مخرجات المعالجة بواسطة الحاسب على الشاشة الخاصة به، أو الانترنت بواسطة الشاشات أو وحدة العرض المرئي[2]، ويكون الدليل باطلاً إذا تحصَّل عليه عن طريق مخالفة القانون، ولهذا الموضوع أهمية بالغة لما يترتب عليه بطلان الدليل من آثار، فإذا كان الدليل الباطل هو الدليل الوحيد فلا يصح الاستناد عليه في إدانة المتهم، فإذ ما شاب التفتيش الواقع على نظم الحاسب عيب فإنه يبطله، والتفتيش الذي يقوم به المحقق بغير الشروط التي نص عليها القانون يعتبر باطلاً بطلاناً مطلقاً ولا يجوز التمسك بما ورد في محضر التفتيش كما لا يجوز للمحكمة أن تعتمد عليه في حكمها[3]. ويقع عبء إثبات الجرائم المعلوماتية على عاتق النيابة العامة، كما أن المدَّعي بالحق الشخصي يشارك النيابة العامة هذا العبء، وفي أحيان أخرى ينقل القانون عبء الإثبات من النيابة العامة إلى عاتق المشتكى عليه[4].

---

(1) Digital Evidence and Computer Crime, by Eoghan Casey, 1st edition Academic Pr. 2000.

(2) أحمد، هلالي عبد اللاه، حجية المخرجات الكمبيوترية في الإثبات الجنائي، ط1، دار النهضة العربية، القاهرة، 1997م.

(3) العكيلي، عبد الأمير، أصول الإجراءات الجنائية في قانون أصول المحاكمات الجزائية، ج1، ط1، مطبعة المعارف، بغداد، 1975م.

(4) صالح، نائل عبد الرحمن، محاضرات في قانون أصول المحاكمات الجزائية، ط1، دار الفكر العربي، عمان، 1997م.

أما في النظم الأنجلو سكسونية التي يُحدد المشرِّع فيها أدلة الإثبات ويُقدر قيمتها الإقناعية، في طليعة هذه الدول التي تتبنى هذا النظام، بريطانيا، التي أصدرت قانون إساءة استخدام الحاسب في عام 1990م، الذي لم يتناول الأدلة الناتجة عن الحاسب، وربما كان السبب هو وجود قانون البوليس والإثبات الجنائي لسنة 1984م، الذي حوى تنظيماً محدداً لمسألة قبول مخرجات الحاسب والانترنت، كأدلة إثبات في المواد الجنائية[1]، وفي الولايات المتحدة الأمريكية تناولت بعض القوانين حجية الأدلة الإليكترونية، وما نص عليه قانون الحاسب لسنة 1984م، الصادر في ولاية (ايوا)، من أن مخرجات الحاسب تكون مقبولة بوصفها أدلة إثبات بالنسبة للبرامج والبيانات المخزنة فيه (المادة 16/أ/716)، كما يتضح من قانون الإثبات الصادر في عام 1983م في ولاية كاليفورنيا، من أن النسخ المستخرجة من البيانات التي يحتويها الحاسب تكون مقبولة بوصفها أفضل الأدلة المتاحة لإثبات هذه البيانات[2]، وفي كندا، يمكن قبول السجلات الناجمة عن الحاسب، إذا توافرت شروط معينة، وتنص المادة (29) من قانون الإثبات الكندي على عدد من الشروط التي يجب توافرها قبل عمل صورة (Copy)، من السجل الذي يُضاف إلى الأدلة، ومن هذه الشروط أن تكون الصورة حقيقية من المدخل الأصلي، وقد قضت محكمة استئناف اونتاريو الكندية في قضية مكميلان (MC Mullen)، بأنه يشترط لكي تكون سجلات الحاسب مقبولة بوصفها نسخاً حقيقية من السجلات الإليكترونية، وأن تكون محتوية على وصف كامل لنظام حفظ السجلات السائد في المؤسسات المالية، كما يمكن أن يتضمن ذلك وصفاً للإجراءات والعمليات المتعلّقة بإدخال البيانات وتخزينها واسترجاعها، حتى يتبين أن المخرج المتحصل من الحاسب موثوق به بشكل

(1) (حسن، سعيد عبد اللطيف، الإثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، الجرائم الواقعة في مجال تكنولوجيا المعلومات، المرجع السابق.

(2) Csonka, peter, Op. cit., p 176 - 177.

كاف[1]. وتنص قواعد الإثبات الفيدرالية الأمريكية، على أن النسخة المطابقة للأصل لها ذات حجية الأصل، أياً كانت الطريقة أو الوسيلة المستخدمة في النسخ، كالطباعة، والتصوير، والتسجيل الميكانيكي، والتسجيل الإليكتروني، بما يسمح بقبول مخرجات الحاسب في الإثبات، والغالب الأعم في القضاء الأمريكي أنه يُعول على قبول دليل السجلات المحتفظ بها على الحاسب[2].

أما في القوانين ذات الاتجاه المختلط، وهي التي تجمع ما بين النظامين اللاتيني والأنجلوسكسوني فيعتمد النظام المختلط على أن يُحدد القانون أدلة معينة لإثبات بعض الوقائع دون بعضها الآخر، أو يشترط في الدليل شروطاً في بعض الأحوال، أو يعطي القاضي الحرية في تقدير الأدلة القانونية، مثل القانون الإجرائي الياباني، وقد حصر المشرِّع الياباني طرق الإثبات المقبولة بما يأتي: (أقوال المتهم، وأقوال الشهود، والقرائن، والخبرة)، أما بالنسبة لأدلة الحاسب والانترنت، فيقرر الفقه الياباني، أن السجلات الإليكترومغناطيسية تكون غير مرئية في حد ذاتها، ولذلك لا يمكن أن تستخدم كدليل في المحكمة، إلا إذا تم تحويلها إلى صورة مرئية ومقروءة عن طريق مخرجات الطباعة لمثل هذه السجلات، وفي مثل هذه الحالة يتم قبول هذه الأدلة الناتجة عن الحاسب والانترنت، سواء كانت هي الأصل أم كانت نسخة من هذا الأصل[3].

وأعطى المشرِّع الأردني النيابة العامة سلطة التحري وجمع الأدلة من خلال قانون أصول المحاكمات الجزائية، وقد نصت المادة (17) منه على أنه:

1 - المدَّعي العام مكلف باستقصاء الجرائم وتعقب مرتكبيها.

---

(1) (أحمد، هلالي عبد اللاه، حجية المخرجات الكمبيوترية في الإثبات الجنائي، المرجع السابق.

(2) حسن، سعيد عبد اللطيف، الإثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، الجرائم الواقعة في مجال تكنولوجيا المعلومات، المرجع السابق.

(3) (عرب، يونس، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، المرجع السابق.

2 – ويقوم بذلك على السواء المدّعون العامّون المختصون وفقاً لأحكام المادة (5) من هذا القانون)، والدليل المتحصل من تفتيش نظم الحاسب والانترنت لا يكون مشروعاً، ويُعتَبر باطلاً إذا تم الحصول عليه بغير الشروط التالية:

الشرط الأول: يجب الحصول على الدليل بصورة مشروعة غير مخالفة لأحكام الدستور ولا لقانون العقوبات[1]، وإن أهم هدف للدستور هو صيانة كرامة الإنسان وحماية حقوقه؛ لذلك تتضمن الدساتير الحديثة نصوصاً تنظم القواعد الأساسية في الاستجواب والتوقيف والحبس والتفتيش وغيرها، بحيث يتقيد المشرِّع بها عند وضع قانون أصول المحاكمات الجزائية، فنص الدستور الأردني في المادة (10) منه على أن: (للمساكن حرمة فلا يجوز دخولها إلا في الأحوال المُبيّنة في القانون، وبالكيفية المنصوص عليها فيه)، ونصت كذلك المادة (18) من الدستور الأردني أيضاً على أنه: (تعتبر جميع المراسلات البريدية والبرقية والمخاطبات الهاتفية سرية فلا تخضع للمراقبة، أو التوقيف، إلا في الأحوال المعينة في القانون)، فهذه النصوص الواردة في الدستور تفرض على المشرِّع عند وضع قواعد الإجراءات الجنائية الالتزام بها وعدم الخروج عنها، وكذلك فإن إجراءات الحصول على الأدلة الجنائية يجب أن تكون ضمن الإطار العام الذي حدده الدستور وإلا فإن الدليل المستمّد بطريق مخالف للأحكام الواردة في الدستور يكون باطلاً بطلاناً مطلقاً لتعلُّقه بالنظام العام، ويجوز لكل ذي مصلحة التمسُّك به كما أن للمحكمة أن تقضي به من تلقاء نفسها، ونرى ضرورة أن يقوم المشرِّع الأردني بتشريع نصوص إجرائية تتكفَّل بحماية الحياة الخاصة المخزونة في الحاسوب والانترنت، بحيث تمنع اقتحام الملفات الشخصية بدون سند قانوني، حماية للحقوق والحريات الفردية التي كفلها الدستور الأردني، بالإضافة إلى المواثيق الدولية.

---

(1) عوض، رمزي رياض، مشروعية الدليل الجنائي في مرحلة المحاكمة وما قبلها، دراسة تحليلية تأصيلية مقارنة، دار النهضة العربية، القاهرة، 1997م

أما جـزاء مخالفة القانون في الحصول على الأدلـة فيترتب عليه جزاءات جنائية أو إدارية فضلاً عن الحكم بالتعويض، فالموظف الذي يعهد إليه القانون بعمل فيتصرف على وجه مخالف يُعد مقصراً في عمله ومخالفاً في واجباته فيستحق المؤاخذة[1]، والمهم هنا هو الجزاء الإجرائي إذ لا شك أن الدليل المستخلص عن طريق ارتكاب جريمة يكون باطلاً بطلاناً متعلقاً بالنظام العام، ومن أمثلة ذلك ما نصت عليه المادة (347) من قانون العقوبات الأردني على أنه: (1 -من دخل مسكن آخر أو ملحقات مسكنه خلافاً لإرادة ذلك الآخر، وكذلك من مكث في الأماكن المذكورة خلافاً لإرادة مَن له الحق في إقصائه عنها عوقب بالحبس مدة لا تتجاوز الستة أشهر)، وكذلك نص المادة (355) من قانون العقوبات الأردني التي جاء فيها: (يُعاقب بالحبس مدة لا تزيد على ثلاث سنوات كل من:

1 - حصل بحكم وظيفته أو مركزه الرسمي على أسرار رسمية وأباح هذه الأسـرار لمن ليس له صلاحية الاطلاع عليها أو إلى من لا تتطلب طبيعة وظيفته ذلك الاطلاع وفقاً للمصلحة العامة.

2 - كان يقوم بوظيفة رسمية أو خدمة حكومية واستبقى بحيازته وثائق سرية أو رسوماً أو مخططات أو نماذج أو نسخاً منها دون أن يكون له حق الاحتفاظ بها أو دون أن تقتضي ذلك طبيعة وظيفته.

3 - .كان بحكم مهنته على علم بسر وأفشاه دون سبب مشروع، ولم يقتصر المشرِّع في حمايته لأسرار الأفراد على الاطلاع عليها بطرق عادية بل شمل حتى الأسرار داخل المراسلات والبرقيات،

فنصت المادة (356) عقوبات أردني على أنه:

---

(1) الطوالبه، على حسن، التفتيش الجنائي على نظم الحاسوب والانترنت، دراسة مقارنة، ط1، عالم الكتب الحديث، اربد، 2004م.

1 - يُعاقب بالحبس من شهر إلى سنة كل شخص ملحق بمصلحة البرق والبريد يُسيء استعمال وظيفته هذه بأن يطّلع على رسالة مظروفه، أو يتلف، أو يختلس إحدى الرسائل أو يفضي بمضمونها إلى غير المرسَل إليه.

2 - ويُعاقب بالحبس مدة ستة أشهر أو بالغرامة حتى عشرين دينار مَن كان ملحقاً بمصلحة الهاتف وأفشى مخابرة اطلع عليها بحكم وظيفته أو عمله، وفي جميع هذه الحالات يرتب العمل المخالف للقانون لمن وقع عليه الحق في التعويض فضلاً عن استحقاق القائم به للعقوبة الجنائية مع وجوب بطلان هذا العمل كونه وليد جريمة، وبالتالي بطلان الدليل الذي استمد منه هذا العمل، لأن ما يُبنى على الباطل يكون باطلاً، ويرى الباحث إمكانية انطباق القواعد التقليدية على هؤلاء المذكورين في النصوص السابقة، في حالة إطلاعهم بحكم وظائفهم على أسرار المواطنين عبر أجهزة الحاسوب أو شبكاته من خلال أدائهم لوظائفهم، لكن يبقى التساؤل على من تم ذكرهم أعلاه كشهود على الجريمة المعلوماتية، فهل هم ملزمون أن يقوموا بطبع ملفات البيانات المخزّنة في ذاكرة الحاسب مفشين للسر، أو الإفصاح عن كلمات المرور السرية، أو الكشف عن الشفرات المدوَّنة بها الأوامر الخاصة بتنفيذ البرامج، لقد اختلف الفقه المقارن في ذلك إلى الاتجاهات التالية:

الاتجاه الأول: يذهب أصحابه إلى أنه ليس من واجب الشاهد، وفقاً للالتزامات التقليدية للشهادة -أن يقوم بما تم ذكره سابقاً - ففي لوكسبورغ، الشاهد ليس مجبراً على التعاون في كل ما يعرفه عند سؤاله أمام المحكمة، وبالتالي من الصعب إجباره على تقديم بيانات يجهلها ولم يقم بإدخالها بنفسه في ذاكرة الحاسوب، وإن كان يستطيع الوصول إليها نظراً لمعرفته

بكلمات المرور السرية[1]، أما إذا تعاون الشاهد على هذا النحو فإن دوره يكون أقرب إلى الخبرة منه إلى الشهادة، وفي ألمانيا، تذهب غالبية الفقه إلى عدم التزام الشاهد بطبع البيانات المخزّنة في ذاكرة الحاسوب، على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب، وفي تركيا لا يجوز إكراه الشاهد لحمله على الإفصاح عن كلمات المرور السرية، أو كشف شفرات تشغيل البرامج المختلفة.

الاتجاه الثاني: ويرى أنصاره أن من الالتزامات التي يجب أن يقوم بها الشاهد، هي طبع ملفات البيانات، أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة، ففي فرنسا يرى جانب من الفقه في غياب النص التشريعي يكون الشاهد مكلفاً بالكشف عن كلمات المرور السرية التي يعرفها وشفرات تشغيل البرامج[2]، ما عدا حالات المحافظة على سر المهنة، فإنه يكون في حل من الالتزام بأداء الشهادة، وفي هولندا يُتيح قانون الحاسب لسلطات التحقيق إصدار الأمر للقائم بتشغيل النظام بتقديم المعلومات اللازمة لاختراقه والولوج إلى داخله، كالإفصاح عن كلمات المرور السرية، والشفرات الخاصة بتشغيل البرامج المختلفة، أو حل رموز البيانات المشفرة[3].

وتنص المادة (113) من قانون الإجراءات الجنائية التشيلي على إمكانية استخدام الأفلام السينمائية، والحاكي (الفونوغراف)، والنظم الأخرى الخاصة بإنتاج الصورة، والصوت، والاختزال، وبصفة عامة أية وسائل أخرى، قد تكون ملائمة، ووثيقة الصلة، وتفضي إلى استخلاص المصداقية، يمكن أن تكون

---

(1) Concil of Europe activites relaled to Information Technology, Data Protection and computer crime, esonka, Peter-Information and Communiction Technology Law - Oat 19 96. Vol. 5. Issue 3. p 177.

(2) رستم، هشام محمد فريد، جرائم الحاسوب كصورة من صور الجرائم الاقتصادية المستحدثة، مجلة الدراسات القانونية، جامعة أسيوط، العدد -17 1995م.

(3) Jeffrey, Sassinsky, Computer Forensices, Op. cit., p 9.

مقبولة كدليل إثبات[1]، ويرى الفقه التشيلي، أن الدليل الناتج عن الحاسب والانترنت، يمكن أن يكون مقبولاً في المحكمة، كدليل كتابي أو مستندي، مثله مثل النظم الحديثة الأخرى لجمع وتسجيل المعلومات، وحجة الفقه التشيلي تستهدف توسيع مظلة الوسائل العلمية الحديثة في الإثبات، لتغطي العناصر الإثباتية الناتجة عن جرائم المعلوماتية[2].

تُعد مراقبة المكالمات السلكية واللاسلكية – تحت رقابة القضاء- من الوسائل الملائمة لضبط ما يفيد في كشف الحقيقة أحياناً، وقد أحاط المشرِّع إجراء المراقبة الهاتفية واللاسلكية بضمانات معينة فلا يجوز إجراؤها إلا بأمر مسبب من القضاء وبصورة مشروعة، والقوة الإثباتية للتسجيلات الصوتية المُسجلة إليكترونياً، فالصوت عند تسجيله إليكترونياً، لا يحتمل الخطأ، ويصعب التلاعب به، ويمكن للخبراء أن يكتشفوا أي تلاعب أو خداع بوسائل تقنية عالية الكفاءة، ومن ثم يمكن القول بأن التسجيل الصوتي المفنط يمكن أن تكون له حجة دامغة في الإثبات[3].

ويمكن باستخدام تكنولوجيا للحاسبات الحديثة والانترنت وطرق الاتصال المعلوماتي السريع، أن يستخدم تسجيل الفيديو لإثبات تُهَم استعمال القسوة أو إساءة استعمال السلطة من قبِل أعضاء الضابطة العدلية ضد المواطنين، كما يمكن استخدامها لتسجيل عمليات القبض والتفتيش وضبط الأدلة والآثار الأخرى الناجمة عن الجريمة تسجيلاً دقيقاً، كما يمكن استخدامها

(1) أحمد، هلالي عبد اللاه، حجية المخرجات الكمبيوترية في الإثبات الجنائي، المرجع السابق.

(2) عوض، رمزي رياض، مشروعية الدليل الجنائي في مرحلة المحاكمة وما قبلها، دراسة تحليلية تأصيلية مقارنة، المرجع السابق.

(3) حسن، سعيد عبد اللطيف، الإثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، الجرائم الواقعة في مجال تكنولوجيا المعلومات، المرجع السابق.

كتقنية عالية الكفاءة لعمل المعاينات اللازمة لمسرح الجريمة[1]، ويشترط الفقه لمشروعية الدليل المستمد من المراقبة والتسجيل توافر الشروط التالية[2]:

1 - إذا لم يكن التسجيل منطويًا على اعتداء على حق يحميه القانون، فيكون الدليل في هذه الحالة مشروعًا، ويمكن للمحكمة أن تستند إليه في قضائها بالإدانة أو بالبراءة.

2 - تحديد دقيق لشخصية الشخص المراد تسجيل أحاديثه أو بريده الإليكتروني كل ما كان ذلك ممكناً في حالة الإنابة للتفتيش.

3 - تحديد نوع الحديث المراد التقاطه، والجريمة المتعلقة بها، والجهة المصرَّح لها بذلك، والمدة الجائز خلالها التقاط الحديث خلالها.

ويمكن استخدام «حاسب الجيب» على أنه «أداة تبرئة» إذ يمكن أن تكون التوقيعات المشفرة من خلاله دليل براءة غير قابل للدحض في مواجهة أية اتهامات باطلة، فلو أن شخصاً ما اتُّهم بأمر معين أو جريمة معينة فبإمكانه أن يُدافع عن نفسه من خلال ما هو مُسجل من أقوال وأفعال في أي وقت[3]. أما البريد الإليكتروني، فعند إرسال رسالة من خلاله فإنه يكون لدى الشخص المستقبل توقيعاً رقمياً (إليكترونياً)، ويكون المستقبل وحده القادر على استعماله، وسيتم تشفير الرسالة، بحيث لن يتمكن من حل شفرتها إلا الشخص المقصود إرسالها إليه، ويمكن لهذه الرسالة أن تكون معلومات من

---

(1) جيتس وآخرون، بيل، المعلوماتية بعد الانترنت (طريق المستقبل)، ترجمة رضوان، عبد السلام، سلسلة عالم المعرفة، المجلس الوطني للثقافة والفنون الآداب، العدد 231، الكويت، مارس 1988م.

(2) البحر، ممدوح خليل، أصول المحاكمات الجزائية، ط1، دار الثقافة، عمان، 1998م.

(3) وهو حاسوب بحجم صغير جداً يمكن وضعه داخل الجيب، ويمكن ربطه كمبيوتر أكبر وبالشبكة العامة بمكتب العمل الخاص، ويمكن للمستخدم أن يحفظ فيه كل ما يريد من أرقام ومواعيد، بالإضافة لاستخدامه ككاميرا تصوير وخلوي، انظر: بيل جيتس، مصدر سابق، ص423-424.

أي نوع، مشتملة على الصوت والفيديو، أو تحويلات بنكية، وسيكون بإمكان متلقِّي الرسالة أن يتأكَّد من أن الرسالة مرسَلة بالفعل من الشخص الذي أرسلها، وتحديد وقت إرسالها بالضبط، وأنها لم تتعرَّض لأي تلاعب، وأن الآخرين لا يستطيعون فك شفرتها، وبالتالي يمكن استخدام هذه المعلومات كحجة في الإثبات الجنائي[1].

ويستخدم التوقيع الإليكتروني في تأمين المعلومات من خلال إدخال أختام توقيت الإرسال في الرسائل المشفرة، فإذا ما حاول شخص ما، أن يُلفق أو يُزور المفترض كتابة أو إرسال الوثيقة فيه فسيكون هذا التلفيق أو التزوير قابلاً للكشف، وسوف يرد ذلك الاعتبار للقيمة الإثباتية للصور الفوتوغرافية والفيديوية، ولقد أضاف علم التصوير للإثبات الجنائي قيمة علمية بما له من أثر في نقل صورة صادقة للأماكن والأدلة إلى كل مَن يعنيه الأمر، اعتماداً على آلة التصوير والأفلام التي لا تعرف الكذب، بيد أنه لا يمكن إنكار الآثار السلبية والخطيرة التي تنشأ عن استخدام هذه الوسائل، لما قد يحدثه في الحياة الخاصة إذا لم توضع له الضوابط الكافية[2]، وتختلف حجية التوقيع الإليكتروني في الإثبات المدني عنه في الإثبات الجنائي، حيث يخضع في الإثبات المدني لقواعد شكلية، أما في الإثبات الجنائي فيخضع تقديره لمطلق سلطة قاضي الموضوع، واقتناعه بصحته وقوته الإثباتية[3]، كما أن وجود نظام تسجيل الدخول في شبكة الانترنت يسمح بتحديد الأشخاص الذين دخلوا أو حاولوا الدخول بعد ارتكاب الفعل الإجرامي، وتعد حالات ضبط مرتكب الفعل متلبسًا نادرة أو أنها وليدة الصدفة، وحتى لو تم ضبطه متلبساً، فقد يرجع

---

(1) حسن، سعيد عبد اللطيف، الإثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، الجرائم الواقعة في مجال تكنولوجيا المعلومات، المرجع السابق.

(2) عابد، عبد الحافظ عبد الهادي، الإثبات الجنائي بالقرائن، دراسة مقارنة، دار النهضة العربية، القاهرة 1998م.

(3) حسن، سعيد عبد اللطيف، الإثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، الجرائم الواقعة في مجال تكنولوجيا المعلومات، المرجع السابق.

ذلك إلى خطأ في نظام الحاسب أو الشبكة أو الأجهزة الأخرى[1]، أو عن طريق مراقبة الشرطة بعد ملاحظة وجود بعض الاعتداءات، والفقه الفرنسي يعتبر انتهاك نظام الأمن لبعض المواقع المحمية، دليل حتمي وقرينة قاطعة على وجود القصد الإجرامي وسوء نية مرتكب الفعل[2]، ويمكن للماسحات الضوئية، وطابعات الليزر أن تكون أداة ارتكاب الجريمة، ففي عام 1994م، قام أحد الأشخاص في مدينة دلاس الأمريكية بتزوير إجازات قيادة سيارات التاكسي باستخدام الماسحات الضوئية، وطابعات الليزر، كما جرت محاولات لإصدار بطاقات التأمين، وأوامر صرف مالية، وبعض أنواع الصكوك من خلال استخدام برمجيات الرسوم المتطورة، وأنظمة الطباعة المتخصصة[3].

وفي إطار مشروعية الأدلة الرقمية، نجد أن قانون الإجراءات الجنائية الفرنسي رغم أنه لم يتضمن أي نصوص تتعلق بمبدأ الأمانة أو النزاهة في البحث عن الحقيقة، إلا أن الفقه والقضاء كانا بجانب هذا المبدأ سواء في مجال التنقيب عن الجرائم التقليدية، أم في مجال التنقيب في جرائم الحاسب والانترنت، كأن يستخدم أعضاء الضابطة العدلية طرقاً معلوماتية في أعمال التصنت على المحادثات الهاتفية، ويشير رأي فقهي فرنسي إلى أن القضاء قد قبل استخدام الوسائل العلمية الحديثة في البحث والتنقيب عن الجرائم تحت تحفظ أن يتم الحصول على الأدلة الجنائية، ومن بينها الأدلة المتحصلة من الحاسوب والانترنت، بطريقة شرعية ونزيهة، ونفس الشيء نجده في سويسرا وبلجيكا[4].

(1) عرب، يونس، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، المرجع السابق.

(2) تمام، أحمد حسام طه، الجرائم الناشئة عن استخدام الحاسوب، (الحماية للحاسوب)، دراسة مقارنة، دار النهضة، القاهرة 2000م.

(3) Flusche, Karl J. – Computer Crime and analysis of Computer evidence – Itain't Just hackers and phreakers anynore- Information System Security – Spring 1998-Vol. 7. Issue 1. P. 24.

(4) أحمد، هلالي عبد اللاه، حجية المخرجات الكمبيوترية في الإثبات الجنائي، المرجع السابق.

وفي بريطانيا، قامت الشرطة بتركيب جهاز تنصت على خط هاتف إحدى الشاكيات بناءً على موافقتها، وقد أجرت الشاكية عدة مكالمات هاتفية مع الشخص الذي كانت الشرطة تشك في ارتكابه الجريمة، وقد تم تسجيل هذه المكالمات التي تضمنت موضوعات تدين المتهم، لكن القاضي استبعد هذه التسجيلات على أساس أنها تمت من خلال شرك خداعي[1].

أما في هولندا، فإذا كانت بيانات الحاسب المسجلة في ملفات الشرطة غير قانونية، فذلك يؤدي إلى نتيجة مؤداها ضرورة محو هذه البيانات، وعدم إمكانية استخدامها كدليل جنائي بسبب مبدأ استبعاد الأدلة غير القانونية[2].

أما في اليابان فقد أصدرت محكمة مقاطعة (KOFV) حكماً أقرت فيه مشروعية التصنت للبحث عن الدليل، حيث ضرورة التحريات، وإمكانية استخدام الإجراءات في التحريات تكون مأخوذة بعين الاعتبار، لكن الفقه الياباني، يرى أن الأدلة الجنائية التي يتم الحصول عليها بطرق مشروعة يجب أن تكون مستبعدة سواء كانت تقليدية أم أدلة حاسب أم أدلة انترنت[3]. ومن أمثلة الطرق غير المشروعة التي يمكن أن تستخدم في الحصول على الأدلة الناتجة عن الجرائم المعلوماتية، الإكراه المادي والمعنوي في مواجهة المتهم المعلوماتي من أجل فك شفرة نظام من النظم المعلوماتية أو الوصول إلى دائرة حل التشفير أو الوصول إلى ملفات البيانات المخزنة، أو التحريض على

---

(1) قايد، أسامة عبد الله، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، المرجع السابق.

(2) إن البيانات التي تجمعها الشرطة عن الأشخاص من أجل حماية الأمن العام يجب أن تبقى تحت سلطة هؤلاء الموظفين بسبب وظيفتهم في حماية الأمن العام، وهي أساس عملهم بهذه البيانات، ومن ثم يجب منع غيرهم من الوصول إليها ممن ليس لهم نفس الاختصاص في إطار الحفاظ على سرية هذه البيانات وحق الخصوصية، انظر: قايد، أسامة عبد الله، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، المرجع السابق.

(3) أحمد، هلالي عبد اللاه، حجية المخرجات الكمبيوترية في الإثبات الجنائي، المرجع السابق.

ارتكاب الجريمة المعلوماتية من قبل أعضاء الضابطة العدلية، كالتحريض على الغش، أو التزوير المعلوماتي، أو التجسس المعلوماتي، والاستخدام غير المصرح به للحاسوب، والتصنت، والمراقبة الإليكترونية عن بُعد[1].

وتُعد من الطرق غير المشروعة أيضاً استخدام التدليس أو الغش أو الخداع في الحصول على الأدلة الرقمية [2]، ولقد صادقت لجنة الوزراء التابعة للمجلس الأوروبي في 1981/1/28م على اتفاقية خاصة بحماية الأشخاص في مواجهة مخاطر المعالجة الآلية للبيانات ذات الطبيعة الشخصية، ومن المحاور المهمة التي تناولتها الاتفاقية ضرورة أن تكون البيانات المضبوطة صحيحة وكاملة ودقيقة، ومستمدة بطرق مشروعة، ومدة حفظها محددة زمنيًا، وعدم إفشائها أو استعمالها في غير الأغراض المخصصة لها، وحق الشخص المعني في التعرف والاطلاع على البيانات المسجلة المتعلقة به وتصحيحها وتعديلها ومناقضتها ومحوها إذا كانت باطلة[3].

ولقد تضمن قانون الشرطة والإثبات الجنائي الإنجليزي لعام 1984م، تحديد الشروط الواجب توافرها في مخرجات الحاسوب لكي تقبل أمام القضاء، وتضمن كذلك توجيهات في كيفية تقدير قيم أو وزن البيان المستخرج عن طريق الحاسب، فأوصت المادة (11) منه[4]، بمراعاة كل الظروف عند تقييم البيانات الصادرة عن الحاسب المقبولة في الإثبات طبقاً للمادة (69) من القانون نفسه، وبوجه خاص مراعاة (المعاصرة) أي ما إذا كانت المعلومات

---

(1) الصغير، جميل عبد الباقي، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، (أجهزة الرادار – الحاسبات الآلية – البصمة الوراثية)، دراسة مقارنة، دار النهضة العربية، القاهرة، 2001م.

(2) شتا، محمد محمد، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، 2001م

(3) الصغير، جميل عبد الباقي، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، (أجهزة الرادار – الحاسبات الآلية – البصمة الوراثية)، المرجع السابق.

(4) Police and Criminal Evidence Act 1984, Op. cit., p 28.

المتعلقة بأمر قد تم تزويد الحاسب بها في وقت معاصر لهذا الأمر أم لا، وكذلك مسألة ما إذا كان أي شخص من المتصلين على أي نحو بإخراج البيانات من الحاسب لديه دافع لإخفاء الوقائع أو تشويهها، وقد نصت المادة (69) على ثلاثة شروط أساسية هي[1]:

1 - يجب ألا يوجد أساس معقول للاعتقاد أن البيان الخاطئ أو غير دقيق، بسبب الاستعمال الخاطئ.

2 - يجب أن تكون جميع المكوّنات المادية للحاسب كانت تعمل بدقة وعلى نحو متوافق كما ينبغي.

3 - إن أياً من الشروط المحددة المتعلقة بالموضوع يجب أن تخضع لتقدير المحكمة، ولقد قضت محكمة الاستئناف الجنائي في إنجلترا بذلك، حيث بيّنت في حكمها كيفية التعامل مع الأدلة المستخرجة من الحاسب، ويتلخص الحكم بما يلي: (أنه يبدو لهذه المحكمة - أنه من الخاطئ رفض أو إنكار أية مزايا أو صلاحيات مقررة وفقاً لقانون الإثبات، يمكن بمقتضاها التوصل عن طريق التقنيات الجديدة والوسائل الحديثة التأكد من صحة وصدق التسجيل، حيث يمكن التثبت من ذلك، وكذلك يمكن التعرف بوضوح على الأصوات المسجلة، والمستخلص أيضاً هو أن الدليل وثيق الصلة بالموضوع، من جهة أخرى، يمكن قبوله، ومن ثم تؤيد المحكمة قبول هذه الأشرطة ويجب أن ينظر دائماً بعين الاعتبار إلى مثل هذا الدليل، وتقدير قيمته في ضوء جميع الظروف بالنسبة لكل قضية) [2].

الشرط الثاني: يجب أن تكون الأدلة الإليكترونية غير قابلة للشك

---

(1) Police and Criminal Evidence Act 1984, Op. cit., p 25..

(2) حسن، سعيد عبد اللطيف، الإثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، الجرائم الواقعة في مجال تكنولوجيا المعلومات، المرجع السابق.

أي يقينية: يُشترط في الأدلة المستخرجة من الحاسوب والانترنت أن تكون غير قابلة للشك حتى يمكن الحكم بالإدانة، ذلك أنه لا مجال لدحض قرينة البراءة وافتراض عكسها إلا عندما يصل اقتناع القاضي إلى حد الجزم واليقين، ويمكن التوصل إلى ذلك من خلال ما يعرض من الأدلة الإليكترونية، والمصغرات الفيلمية، وغيرها من الأشكال الإلكترونية التي تتوافر عن طريق الوصول المباشر، أم كانت مجرد عرض لهذه المخرجات المعالجة بواسطة الحاسب على الشاشة الخاصة به أو على الطرفيات، وهكذا يستطيع القاضي من خلال ما يعرض عليه من مخرجات إليكترونية، وما ينطبع في ذهنه من تصورات واحتمالات بالنسبة لها، أن يحدد قوتها الاستدلالية على صدق نسبة الجريمة المعلوماتية إلى شخص معين من عدمه.

ونصت بعض قوانين الولايات في أمريكا، على أن النسخ المستخرجة من البيانات التي يحتويها الحاسب تُعد من أفضل الأدلة المتاحة لإثبات هذه البيانات، وبالتالي يتحقق مبدأ اليقين لهذه الأدلة، وتنص القواعد الفيدرالية على أن: (الشرط الأساسي للتوثيق أو التحقُّق من صحة أو صدق الدليل، كشرط مسبق لقبوله، هو أن يفي بإمارة أو بينة كافية لأن تدعم اكتشاف (أو الوصول) إلى الأمور التي تتصل بالموضوع بما يؤيد الادعاءات أو المطالبة المدعي بها) [1].

ويقرر الفقه الياباني قبول الأدلة المستخرجة من الحاسوب التي تم تحويلها إلى الصورة المرئية سواء كانت هي الأصل أم كانت نسخاً مستخرجة عن هذا الأصل، وذلك استناداً على الاستثناءات التشريعية المنصوص عليها في المادة (323) من قانون الإجراءات الجنائية الياباني، ففي هذه الحالة يتحقق اليقين الذي يبنى عليه الحكم الجنائي، كما يمكن أن يتحقق اليقين لهذه المخرجات أيضاً من خلال التقارير التي يقدمها الخبراء، وفي تشيلي

---

(1) حسن، سعيد عبد اللطيف، الإثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، الجرائم الواقعة في مجال تكنولوجيا المعلومات، المرجع السابق.

ينص أحد القوانين الخاصة بالحاسب على قبول السجلات الممغنطة للحاسوب وكذلك النسخ الناتجة عنها، ومعنى ذلك أن هذه السجلات وصورها تحقق اليقين المنشود لإصدار الأحكام الجنائية، كما يتحقق هذا اليقين أيضاً عن طريق تقارير الخبراء الصادرة في عناصر معالجة البيانات كما وارد في المادة 221 من قانون أصول المحاكمات الجزائية التشيلي[1].

واعتبر المشرّع الأردني نظام المعالجة الإليكتروني مؤهلاً لإثبات تحويل الحق مما يسهل على المحقق ضبط الدليل الإليكتروني وذلك من خلال نص المادة (21) من قانون المعاملات الإليكترونية رقم (85) لسنة 2001م، والتي جاء فيها بأن:

(أ - يُعتبر نظام المعالجة الإليكتروني مؤهلاً لإثبات تحويل الحق في السند تطبيقاً لأحكام المادة (20) من هذا القانون إذا كان ذلك النظام يسمح بإنشاء السند الإليكتروني وحفظه، وتحويله، وذلك بتوافر الشرطين التاليين مجتمعين:

1 - إذا كانت النسخة المعتمدة من السند القابل للتحويل محددة بصورة غير قابلة للتغيير وذلك مع مراعاة أحكام الفقرة (ج) من هذه المادة.

2 - إذا كانت النسخة المعتمدة من السند تدل على اسم الشخص الذي تم سحب السند لمصلحته وأن السند قابل للتحويل وتضمنت اسم المستفيد.

ب - تُرسل النسخة المعتمدة وتُحفظ من قبل الشخص الذي يملك الحق فيها أو الشخص المودعة لديه لمصلحة صاحب الحق في السند.

---

(1) أحمد، هلالي عبد اللاه، حجية المخرجات الكمبيوترية في الإثبات الجنائي، المرجع السابق.

ج - 1 - تعتمد النسخ المأخوذة عن النسخة المعتمدة التي حدث عليها تغيير أو إضافة بموافقة من الشخص الذي يملك حق التصرف في السند.

2 - يؤشر على كل نسخة مأخوذة من السند بأنها معتمدة أو غير معتمدة.

3 - تُعرف كل نسخة مأخوذة من النسخة المعتمدة بأنها نسخة مطابقة للنسخة المعتمدة. يتضح من هذا النص إمكانية إثبات الحق مما يُمكن المحقق من استخدام هذه الوسائل أيضًا بالإضافة للوسائل السابق الإشارة إليها في تفتيش نظم الحاسوب والانترنت.

الشرط الثالث: إمكانية مناقشة الأدلة الإليكترونية المستخرَجة من الحاسوب والانترنت: ويعني مبدأ وجوب مناقشة الدليل الجنائي بصفة عامة أن القاضي لا يمكن أن يؤسس اقتناعه إلا على العناصر الإثباتية التي طرحت في جلسات المحاكمة وخضعت لحرية مناقشة أطراف الدعوى[1]، وهذا يعني أن الأدلة المتحصلة من جرائم الحاسوب والانترنت سواء كانت مطبوعة أم بيانات معروضة على شاشة الحاسوب، أم كانت بيانات مدرَجة في حاملات البيانات، أم اتخذت شكل أشرطة وأقراص ممغنطة، أو ضوئية، أو مصغرات فيلمية، كل هذه ستكون محلاً للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة، وعلى ذلك فإن كل دليل يتم الحصول عليه من خلال بيئة تكنولوجيا المعلومات، يجب أن يُعرض في الجلسة ليس من خلال ملف الدعوى في التحقيق الابتدائي، لكن بصفة مباشرة أمام القاضي، وهذه الأحكام تنطبق على كافة الأدلة المتولدة عن الحاسبات، وأيضاً بالنسبة لشهود الجرائم المعلوماتية الذين يكون قد سبق أن سمعت أقوالهم في التحقيق الابتدائي،

---

(1) قرار محكمة النقض المصرية في 1986/11/20م، رقم 179، المبادئ القانونية، ص 943.

فإنه يجب أن يعيدوا أقوالهم مرة أخرى من جديد أمام المحكمة[1]، كذلك فإن خبراء الأنظمة المعلوماتية على اختلاف تخصصاتهم[2]، ينبغي أن يمثلوا أمام المحاكم لمناقشتهم، أو مناقشة تقاريرهم التي خلصوا إليها لإظهار الحقيقة وكشفاً للحق.

ومن القواعد العامة المستقرّة في القانون الجنائي عدم قبول البينة السماعية أمام المحاكم الجنائية، إلا في حالات استثنائية حصرها القانون بشروط مشددة[3]، ويُعزى عدم قبول البينة السماعية إلى استحالة استجواب ومناقشة الشاهد الأصلي بواسطة المحكمة والدفاع، ولاستثناءات البينة السماعية علاقة بمناقشة حجية الأدلة الجنائية الإليكترونية، على سبيل المثال، لقد تضمّنت القواعد الفيدرالية الأمريكية نصاً يعتبر السجلات والبيانات المنظمة بدقة بينة مقبولة أمام المحاكم الجنائية استثناءً للبينة السماعية، وبناءً على تلك القواعد تُعد التقارير والمعلومات والبيانات المحفوظة في أي شكل، وكذلك الوقائع والأحداث والآراء ونتائج التحاليل المنقولة بواسطة أصحاب المعرفة والخبرة في نطاق الأنشطة والممارسات المنظمة بيّنة مقبولة أمام المحاكم الجنائية لكونها بيانات أكثر دقة ومحفوظة بأسلوب علمي يختلف عن غيرها من الأدلة السماعية، والأدلة الجنائية الإليكترونية من هذا القبيل لكونها معدة بعمليات حسابية دقيقة لا يتطرق إليها الشك ويتم حفظها آلياً بأسلوب علمي[4].

---

(1) أحمد، هلالي عبد اللاه، التزام الشاهد بالإعلام في الجرائم المعلوماتية، دراسة مقارنة، النسر الذهبي، القاهرة، 2000م.

(2) طلبة، محمد فهمي وآخرون، دائرة المعارف الحاسب الإليكتروني، مجموعة كتب دلتا، مطابع المكتب المصري الحديث، القاهرة، 1991م.

(3) وهناك استثناءات على هذه القاعدة نص عليها القانون انظر: المواد (156، 157، 162) من قانون أصول المحاكمات الجزائية الأردني.

(4) البشري، محمد الأمين، الأدلة الجنائية الرقمية، مفهومها ودورها في الإثبات، المجلة العربية للدراسات الأمنية والتدريب، المجلد 17، العدد 33، السنة 17، الرياض، أبريل 2002م.

وحول إمكانية ضبط الأدلة ومشروعيتها إذا كانت النهاية الطرفية للنظام المعلوماتي في منزل آخر غير منزل المتهم، فقد أجاز قانون جريمة الحاسب الهولندي في المادة (25/أ) منه، إمكانية امتداد تفتيش المسكن إلى تفتيش نظام آلي... موجود في مكان آخر بغية التوصل إلى بيانات يمكن أن تفيد بشكل معقول.. في كشف الحقيقة وإذا ما وجدت هذه البيانات يجب تسليمها، وبالتالي أجاز المشرِّع للقائم بالتفتيش سلطة تسجيل البيانات الموجودة في النهاية الطرفية التي يتصل بها النظام المعلوماتي دون التقيُّد بالحصول على إذن مسبق بذلك من المحقق المختص، إلا أن هذه السلطة غير مطلقة بل هي مقيَّدة بقيود ثلاثة هي[1]:

1 - ألا تكون النهاية الطرفية المتصل بها الحاسب موجودة ضمن إقليم دولة أخرى حتى لا يؤدي الاتصال بها إلى انتهاك لسيادة الدولة الإقليمية.

2 - أن تحتوي النهاية الطرفية المتصل بها الحاسوب على بيانات ضرورية بصورة كافية لظهور الحقيقة.

3 - أن يحل قاضي التحقيق محل الشخص صاحب المكان الذي ينبغي تفتيشه بصورة مؤقتة.

ويُلاحظ أن المادة (25/أ) من قانون الحاسب الهولندي استثنت هذه الحالة، فيمكن الحصول على الأدلة حتى لو كانت في إقليم دولة أخرى بواسطة الاتفاقيات الدولية الخاصة بالتعاون الأمني والقضائي والخاصة بالتفتيش وضبط الأدلة، وأخيرًا فإن متحصلات الجريمة المعلوماتية [2]، التي يتم ضبطها يجب أن تُعرَض على القاضي المختص بكافة مفرداتها وعناصرها،

---

(1) عفيفي، عفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، 2003.

(2) أحمد، هلالي عبد اللاه، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دراسة مقارنة، المرجع السابق.

وذلك لأن حيادية القاضي توجب عليه أن لا يقيم قضاءه إلا على ما طرح أمامه وكان موضوع الفحص والتحقيق والمناقشة. ويترتب على مناقشة أدلة الحاسب والانترنت:

النتيجة الأولى: عدم جواز أن يقضي القاضي في الجرائم المعلوماتية بناءً على معلوماته الشخصية.

والنتيجة الثانية: ضرورة التأهيل التقني والفني للقضاة لمواكبة المناقشة العلمية لأدلة الحاسوب والانترنت بشكل يتماشى مع التقارير التي تم تقديمها في المؤتمرات الخاصة بجرائم الحاسب والانترنت.

المبحث الخامس

حجية الأدلة الجنائية في الإثبات

يعتمد ضبط الجريمة وإثباتها في المقام الأول على جمع الأدلة التي حدد المشرِّع وسائل إثباتها على سبيل الحصر، وذلك لما فيها من مساس بحرية الأفراد وحقوقهم الأساسية، فلا يجوز أن تخرج الأدلة التي يتم تجميعها عن تلك التي اعترف لها المشرِّع بالقيمة القانونية، وتتمثّل في وسائل الإثبات الرئيسية وفي المعاينة والخبرة والتفتيش وضبط الأشياء المتعلقة بالجريمة، أما غيرها من وسائل الإثبات كالاستجواب والمواجهة وسماع الشهود فهي مرحلة تالية من إجراءات التحقيق وجمع الأدلة، ولما كنا بصدد تناول الجريمة المعلوماتية وما تُثيره من مشكلات إجرائية، فسنتعرَّض للمشكلات القانونية التي يُثيرها إثبات هذه الجرائم دون غيرها من الإجراءات كالاستجواب والمواجهة وسماع الشهود، لأن هذه الأخيرة تتم في مواجهة البشر[1].

المطلب الأوّل

حجية المخرجات الإليكترونية في الإثبات

تخضع المحررات كغيرها من الأدلة التي تُقدم أثناء نظر الدعوى إلى تقدير المحكمة حيث يسود مبدأ حرية القاضي في تكوين عقيدته، وهو ما يختلف فيه القاضي المدني حيث يتقيَّد هذا الأخير بطرق معينة في الإثبات، فالقاضي الجنائي له مطلق الحرية في تقدير الدليل المطروح أمامه، وله أن

(1) رستم هشام، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني مجلة الأمن والقانون، دبي العدد (2)، 1999م.

يأخذ به أو يطرحه ولا يجوز تقييده بأي قرائن أو افتراضات [1].

ولما كانت المحررات أحد الأدلة التي قد يلجأ إليها القاضي في الإثبات فهي تخضع كغيرها من الأدلة لتقدير المحكمة، إلا إذا كان الإثبات متعلقاً بمواد غير جنائية، ففي هذه الحالة يكون على القاضي الجنائي أن يتقيَّد بطريق الإثبات المحددة في ذلك الفرع من القانون مثال ذلك حق الملكية في جريمة السرقة، والعقود التي تثبت التصرف في الحق في جريمة خيانة الأمانة أو صفة التاجر في جريمة التفالس بالتدليس [2].

وهنا تثور مشكلة مدى حجية المخرجات الإليكترونية في الإثبات الجنائي في هذه الحالات، فللمخرجات الإليكترونية أنواع مختلفة، فهي تتنوع بين مخرجات ورقية، ومخرجات ورقية وهي المعلومات المسجلة على الأوعية الممغنطة كالأشرطة والأقراص المرنة Floppy Disk القرص الصلب Hard Disk وغيرها من الأوعية التي أصبحت في تطور مستمر حتى وصلت إلى أقراص الـ flash discs التي أصبحت تتميز بسعات كبيرة للتخزين، خاصة أنه تواجهنا مشكلة أساسية تتعلق بصعوبة التمييز بين المحرر وصورته أو بين الأصل والصورة، ذلك لأننا نتعامل مع بيئة إليكترونية تعمل بالنبضات والذبذبات والرموز والأرقام وهو ما يستحيل معه تطبيق القواعد الخاصة بالمحررات العرفية [3].

ولا يزال المشرِّع في بعض الدول العربية عازفاً عن التدخل التشريعي في هذه المسألة فلا نجد بداً من تطبيق القواعد العامة في هذا الصدد، ولما كان ذلك، فالمشرِّع الليبي لايزال يعتمد على مبدأ سيادة الدليل الكتابي على غيره

(1) سلامة، مأمون، الإجراءات الجنائية في التشريع الليبي، ج 2، ط2000، منشورات المكتبة الجامعة، القاهرة.

(2) سلامة، مأمون، الإجراءات الجنائية في القانون المصري، ج 2، ط2000 م، دار النهضة العربية، مصر.

(3) شرف الدين، احمد، حجية الرسائل الإليكترونية في الإثبات، شبكة المعلومات القانونية العربية، East Law. com – 2007

من الأدلة ولا يجوز الاعتماد على الدليل غير الكتابي في غير المسائل الجنائية، إلا على سبيل الاستئناس، ولا يخفى ما يؤدي ذلك من تقييد للقاضي الجنائي لأن الإثبات في المسائل الجنائية كثيراً ما يعتمد على مسائل غير جنائية، وهو ما سبقت الإشارة إليه عند تناول جريمة التزوير في هذا البحث التي اعتمدت على مدى اعتبار هذه الأوعية من قبيل المستندات أو المحررات موضوع جريمة التزوير، فمواجهة الجرائم المعلوماتية لا تتأتى إلا عن طريق نظام قانوني متكامل أهم عناصره التدخل لضبط المعاملات والتجارة الاليكترونية وصفاء الحجية القانونية على المستندات الإليكترونية شأنها شأن المستندات الورقية، حتى يُتاح للقاضي الجنائي الاعتماد عليها واتخاذها دليلاً جنائياً، كغيره من الأدلة، وقد كان المشرِّع التونسي من السباقين بين أقرانه على المستوى العربي في هذا المجال، حيث صدر في تونس قانون التجارة والمعاملات الإليكترونية الذي اعترف للمستندات الإليكترونية سنة 2000 م بحجيتها في الإثبات، كما أصدرت إمارة دبي قانون التجارة الإليكترونية سنة 2002م، وتبعهما بعد ذلك المشرِّع المصري سنة 2004م الذي أصدر قانون نظم التوقيع الإليكتروني، وتجدر الإشارة في هذا الصدد إلى القانون العربي النموذجي السابق الإشارة إليه سنة 2003م، وكل هذه القوانين أعطت للمستند الإليكتروني ذات الحجية التي يتمتع بها المحرر الورقي، تجدر الإشارة أيضاً إلى أن لجنة الأمم المتحدة للقانون التجاري الدولي United Nation Commission on International Trade Law (UNCITRAL) على هذه الحجية وقد كان ذلك سنة 2000م أما القانون العربي النموذجي فنص في المادة الأولى منه على تعريف الكتابة بأنها كل (عملية تسجيل للبيانات على وسيط لتخزينها)، والمقصود بالوسيط في هذه الحالة هو الوسيط الإليكتروني؛ لأن الوسيط الورقي المتمثل في الأوراق التقليدية لا يحتاج إلى تعريف، وإن كنا نتحفَّظ على استخدام عبارة الوسيط دون تحديده بالإليكتروني، مادام الأمر متعلقاً بالتجريم والعقاب، أما المادة 6 من قانون الاونسترال النموذجي والمشرِّع التونسي يُعد سباقاً إلى اللحاق بهذا التطور التشريعي فإن المشرِّع السنغافوري أصدر قانوناً للإثبات أقر فيه حجية المستندات المعلوماتية في الإثبات منذ سنة 1997م وهو ما يبين مدى تأخر المشرِّع الليبي في مواكبة هذا التطور.

المطلب الثاني

الإثبات الرقمي في المسائل المدنية والتجارية والمصرفية

مما لا شك فيه أن الكتابة من بين الأدلة القانونية منزلة متقدمة وتحديداً في المسائل المدنية والتصرفات العقدية، ففي النظام اللاتيني كما نرى القانونين الفرنسي والمصري تُمثل الكتابة أقوى الأدلة، في حين بقي للشهادة منزلة متقدمة في النظام الأنجلو أمريكي كما هو واضح في القانونين الأمريكي والبريطاني مع اتجاه فيهما بدرجات متفاوتة بينهما إلى إعلاء شأن الكتابة والتضييق من شأن الشهادة أو ما يُعبر عنه بالبينة الشخصية (1).

ووفقاً لأغلب القوانين العربية فإن أدلة الإثبات أو البينات على ستة أنواع:

1 - الأدلة الكتابية.

2 - الشهادة.

3 - القرائن.

4 - الإقرار.

5 - اليمين.

6 - المعاينة والخبرة.

أما الأدلة الكتابية فتنقسم إلى:

1 - المستندات الرسمية.

2 - المستندات العرفية.

---

(1) أحمد، هلالي عبد اللاه، التزام الشاهد بالإعلام في الجرائم المعلوماتية، دراسة مقارنة، المرجع السابق.

أما المستندات الرسمية فتشمل المسندات التي يُنظمها الموظفون المختصون بتنظيمها، وتسبغ الرسمية على محتواها كله ولا يطعن فيها إلا بالتزوير، وتشمل أيضاً المسندات التي يُنظمها أصحابها ويصدقها الموظفون الذين من اختصاصهم تصديقها، وتكون الرسمية بالنسبة لهذا النوع محصورة في التاريخ والتوقيع فقط. أما المستندات العرفية فتشمل أي سند يتضمن توقيع من صدر عنه أو خاتمه أو بصمة اصبعه ولا ينطبق عليها وصف السند الرسمي.

ولو نظرنا إلى القواعد العامة في الإثبات في النظام القانوني الأردني لا تقبل أية مستندات أو محررات غير موقّعة من منظمها، ولا تقبل الاحتجاج بالسندات العادية – ما لم يقر الخصم بها – إلا عن طريق إبرازها من قِبل منظمها، وتنحصر المستندات غير الموقّعة بما حدده حصراً قانون البينات وفي حدود ما قرره لها من أحكام، وعلى ذلك فإن كشوف الحسابات غير الموقعة وغير المبرزة من منظمها ليست حجة وكذا الفواتير أو المستندات المحاسبية أو غيرها، وفي ذلك قضت محكمة التمييز الأردنية: (أن الفواتير التي تخلو من التوقيع أو لم تعزز بإقرار أو بينة لا تصلح حجة على الخصم، ولذلك لا يؤخذ بالدفع المجرد من الدليل) [1] .

المطلب الثالث

دور تقنية المعلومات على وسائل التعاقدات المدنية والمصرفية

لقد أمكن استغلال وسائل تقنية المعلومات في إبرام العقود المختلفة وتبادل البيانات التي تتصل بالذمة المالية، وأُتيح بفضل ربط الحواسيب وشبكة الانترنت، التعاقد الفوري بين شخصين غائبين مكاناً وإجراء مختلف

(1) عرب، يونس، جرائم الكمبيوتر والانترنت، موسوعة القانون وتقنية المعلومات، المرجع السابق.

التصرفات القانونية، وإذا كانت التشريعات المدنية والتجارية قد وقفت فيما سبق أمام فكرة التعاقد بواسطة التلكس أو الهاتف، فإنها من جديد تقف أمام مسالة استخدام نظم الكمبيوتر وشبكات المعلومات في التعاقد وأمام مسائل الإثبات فيما أنتجته الحواسيب والشبكات من مخرجات. وبحث مدى حجية مستخرجات الحاسب والبريد الإلكتروني وقواعد البيانات المخزنة داخل النظم وغيرها. واستخدام وسائل تقنية المعلومات لإبرام العقود والتصرفات القانونية وتبادل البيانات وإجراء عمليات تتصل بالذمة المالية أثار ويُثير العديد من الإشكالات حول مدى اعتراف القانون [1]، وتحديداً قواعد التعاقد، بهذه الآليات الجديدة للتعبير عن الإيجاب والقبول وبناء عناصر التعاقد، كما أثارت وتُثير إشكالات في ميدان الإثبات بكون النظم القانونية قد حددت الأدلة المقبولة وحددت قواعد الاحتجاج بها وسلامة الاستدلال منها على نحو ما أوضحنا أعلاه بشان النظام القانوني الأردني. وفي خضم البحث في قانونية التعاقد بالطرق الإليكترونية وحجية مستخرجات الوسائل التقنية في الإثبات، ظهرت التجارة الإليكترونية كنمط جديد من أنماط التعامل التجاري، لا في ميدان البيع والشراء وإنما في ميادين التعاقد كافة كعقود التأمين والخدمات وغيرها. وأثارت وتُثير التقنية العالية وتحديداً محتواها الفني والمعرفي تحديات كبيرة في ميدان نقل التكنولوجيا والتبادل الفني والمعرفي والتزام مورد التكنولوجيا ومتلقيها، وأظهرت التقنية تحديات قانونية تستلزم التنظيم بالنسبة لعقود تقنية المعلومات، التوريد والبيع والصيانة والتطوير ورخص الاستخدام، وبالنسبة لعقود الوكالات التجارية والتوزيع، وعقود اشتراكات المعلوماتية وخدمات الاتصال، وكان - وسيبقى إلى حين - أوسع اثر لها في حقل التجارة الإليكترونية والتعاقد الإليكتروني.

ولم يتوقف تأثير تقنية المعلومات على قواعد التعاقد والإثبات، بل امتد إلى كل ما يتصل بآليات الوفاء بالالتزامات العقدية وفي مقدمتها آليات الدفع

---

(1) البريري، صالح أحمد، دور الشرطة في مكافحة جرائم الإنترنت في إطار الاتفاقية الأوروبية، الموقعة في بودابست في 2001/11/23 - www.arablawinfo.com

النقدي وأداء الالتزامات المالية محل التعاقد، وفي هذا الإطار أفرزت تقنية المعلومات وسائل حديثة لتقديم الخدمات المصرفية وإدارة العمل البنكي، أبرزها ظهر في حقل أنظمة الدفع الإليكتروني والدفع على الخط وإدارة الحسابات عن بعد، كما حدث بفعل التقنية شيوع بطاقات الدفع والائتمان المالية، ويشيع الآن مفهوم المحفظة والبطاقة الماهرة التي تُمهد إلى انتهاء مفهوم النقد الورقي والمعدني، وتفتح الباب أمام مفهوم النقد الإليكتروني أو الرقمي. إلى جانب ذلك تطورت وسائل تداول الأوراق المالية وخدماتها، فظهرت فكرة التعاقد الإليكتروني والتبادل الإليكتروني للأوراق إلى جانب الاعتماد شبه الكلي في أسواق المال على تقنيات الحوسبة والاتصال في إدارة التداول وقيده وإثبات علاقاته القانونية. ويشيع الآن مصطلح البنوك الإليكترونية التي تنفذ خدماتها المصرفية - بل وخدمات ذات محتوى غير مصرفي ضمن توجه نحو الشمولية [1].

(1) حجازي، سهير، التهديدات الإجرامية للتجارة الإليكترونية، مركز البحوث والدراسات، شرطة دبي بدولة الإمارات العربية المتحدة، 2005م.

المبحث السادس

الاتجاه التشريعي بشأن أدلة الإثبات الحديثة وحجيتها

لقد اتجهت النظم القانونية والقضائية والفقهية بوجهٍ عام إلى قبول وسائل الإثبات التي توفر من حيث طبيعتها موثوقية في إثبات الواقعة وصلاحية للدليل محل الاحتجاج، وتُحقق فوق ذلك وظيفتين: إمكان حفظ المعلومات لغايات المراجعة عند التنازع، التوسط في الإثبات عن طريق جهات الموثوقية الوسيطة أو سلطات الشهادات التعاقدية، ومن هنا قبل نظام (سويفت) التقني لغايات الجوالات البنكية - وكذا نظامي شيبس وشابس ونحوهما - وكذلك قبل التلكس لتحقيقهما هذه الطبيعة والوظائف، في حين بقي الفاكس خارج هذا الإطار ومجرد دليل ثبوت بالكتابة أو بينة مقبولة ضمن شرائط خاصة، ومن هنا أيضا أثارت وتُثير الرسائل الإليكترونية عبر شبكات المعلومات كالانترنت والرسائل المتبادلة عبر الشبكات الخاصة والبريد الإليكتروني مشكلة عدم تحقيق هذه الوظائف في ظل غياب المعايير والمواصفات والتنظيم القانوني الذي يُتيح توفير الطبيعة المقبولة للبينات وتحقيق الوظائف التي تُجيز قبولها في الإثبات [1].

وقد خضعت القواعد القانونية للتعاقد والإثبات في النظم المقارنة إلى عملية تقييم في ضوء مفرزات تقنية المعلومات وتحدياتها، وذلك من أجل تبين مدى تواثم النصوص القائمة مع ما أفرزته وسائل الاتصال الحديثة وتحديداً شبكات المعلومات بأنواعها (انترنت، انترنت، اكسترانت)، باعتبار أن القواعد القائمة في نطاق التشريعات عموماً وفي غير فرع من فروع القانون تتعامل مع عناصر الكتابة والمحرر والتوقيع والصورة طبق الأصل و... الخ من مفاهيم

(1) عرب، يونس، جرائم الكمبيوتر والانترنت، موسوعة القانون وتقنية المعلومات، المرجع السابق.

ذات مدلول مادي. وقد أدت عملية التقييم هذه إلى اتخاذ تدابير تشريعية في أكثر من دولة، فعلى الصعيد العالمي كان للجنة اليونسترال في الأمم المتحدة وقفة مبكرة حيث أنجزت القانون النموذجي للتجارة الإليكترونية لعام 1996 الذي عالج من بين ما عالج مسائل التواقيع الإليكترونية وقرر وجوب النص على قبول التوقيع الإليكتروني كوسيلة للتعاقد وإثبات الانعقاد، ولم يحدد قانون اليونسترال معنى معيناً للتوقيع الإليكتروني أو معياراً معيناً لمسائله الإجرائية واكتفى بالمبادئ العامة القائمة على فكرة إيجاد وسيلة تكنولوجية تحقق نفس المفهوم والغرض الذي تحققه التواقيع العادية. وضمن هذا التوجه سارت العديد من التشريعات في أوروبا وأمريكا وشرق أسيا [1].

أما عن الاتجاه التشريعي العربي للتعامل مع تحديات الوسائل الالكترونية في الإثبات، فان البناء القانوني للتشريعات العربية عموماً في حقلي التعاقد والإثبات لم يعرف الوسائل الإليكترونية وتحديداً تلك التي لا تنطوي على مخرجات مادية كالورق، وجاء مبناه قائماً - بوجه عام مع عدد من الاستثناءات - على فكرة الكتابة، المحرر، التوقيع، الصورة، التوثيق، التصديق، السجلات، المستندات، الأوراق ... الخ، وجميعها عناصر ذات مدلول مادي وإن سعى البعض إلى توسيع مفهومها لتشمل الوسائل التقنية، وهي وإن كان من الممكن شمولها الوسائل التقنية ذات المستخرجات التي تتوفر لها الحجية، فإنها لا تشمل الوسائل ذات المحتوى الإليكتروني البحت (طبعاً بشكل مجرد بعيداً عن الحلول المقررة تقنياً وتشريعياً في النظم المقارنة التي نظّمت هذا الحقل).

والتحديد القانوني للرّسائل الإليكترونية يُثير السّؤال حول ما إذا كانت قوانين الإثبات العربية القائمة تنظم وتحكم المعلومات المتبادلة إلكترونياً (electronically) مثلما تنظم وتحكم المستندات والرسائل والمخاطبات الصادرة عن طريق الوسائل الورقية التّقليدية. فتعبير «رسالة إليكترونية»

---

(1) عرب، يونس، صور الجرائم الإلكترونية واتجاهاتها تبويبها ورقة عمل سنة 2006م.

يَعْني المعلوماتَ المدخلة، المرسلَة، المستلمة أو المخَزنةَ بالوسائلِ الإليكترونيةِ، ويشمل ذلك - لا بشكل حصري - البيانات إليكترونية المتبادلة، بريد إليكتروني، برقية، تلكس.. ونجد العديد من التّشريعات تنظم وتستخدم وتشير إلى تعبيرات مثل «كِتابَة»، «توقيع»، «وثيقة»، «أصلي»، «نسخة مطابقة»، «نشر»، «ختم»، «سجل»، «ملف»، «طبعة» «سجل»، «يُسلّم»، الخ. ومن المهم ابتداء التنبه إلى أن المقصود بالرسائل الإليكترونيةِ الشكل إليكتروني أو الرقمي ولَيسَ الشّكلَ الورقيَ اللاحقَ حينما يتم استخراج الرسائل الإليكترونية (طباعتها) على الورق. فإذا أخضعنا هذه الحقائق للتحليل نجد أن التعاريف المستقرة بالمفاهيم القانونية والعرفية والقضائية تعرف الكِتابَة بما يفيد أنها يجب أَن تكون نتيجةَ فعلٍ يدٌ شخص أو بالطّباعة. وتعرف الطباعة بأنها يَجِبُ أَنْ تكون نتيجة الفعلِ بإفراغ الرسالةِ على «ورقة». من هنا لا يشمل ذلك الرسائل الإليكترونية. وتعرف التوقيع بأنه يَتضمّنُ قيام شخصٍ بفعل «التوقّيعُ» أي وضع الرمز الكتابي الدال على شخصيته، وهذا الفعل لا يشملِ التحديد الرقمي الدال على الشخص في بيئة التجارة والأعمال الإليكترونية. كما أن مفهوم الوثيقة يتعلق بالكتابة «ومن هنا تكون محصورة بالوثائقِ الورقية. وبالتالي فإن تعبير «كِتابَة» لا يشمل الرسائل إليكترونيةِ. وهذا ينطبق على التعابير الأخرى، مثل «وثيقة»، «توقيع»، الخ. باعتبارها محصورة بالمظاهر المادية الورقية. ومن جهة أخرى لا يوجد في تعاريفِ القاموس المكافئة ما يُتيح (وإن كان لا يمنع في بعضها) لهذه التعبير أَنْ تَتضمّنَ مفهوم الرسائل إليكترونية والتواقيع الرقمية. وكخلاصة لهذا التحليل فانه يتعين إزالةِ التناقض وعدم الموائمة بين الرّسائل الإليكترونيةِ ونظيراتها في البيئة الورقة أو المادية، وهو ما يتركنا أمام الخيارات التالية: - إما ترك الأمر للقضاء، وأثر ذلك احتمال صدور قرارات قضائية متناقضة وفوات وقت طويل - لا ينسجم وعصر المعلومات فائق السرعة - قبل استقرار الاتجاه القضائي مع مخاطر اعتبار بعض القراراتِ عدم وجود حلول تشريعية من قبيل النقص التشريعي. وهذا قد يؤثر على مستقبل التنظيم القانوني للتجارة والأعمال

الإليكترونية بل ومستوى تطورها. أو خيار تعديل التشريعات القائمة، لجهة اعتبار تعبيرات الكتابة والوثيقة والتوقيع و... الخ شاملة للرسائل والتواقيع الإليكترونية، ومشكلة ذلك سعة نطاق التعديل وصعوبته والأهم حاجته إلى دراسة شاملة لكافة تشريعات النظام القانوني. أو خيار إصدار تشريع خاص بمفهوم الرسائل الإليكترونية وهي طريقة إحالة إلى سائر التشريعات الأخرى بحيث ينص على أن مفهوم الكتابة والوثيقة والتوقيع وغيرها بأنه يشمل الرسائل والتواقيع الإليكترونية أينما وردت، وهذا الخيار يمثل ما يمكن تسميته بتشريع أولي لا يعالج مسائل التجارة والأعمال الإليكترونية بشكل شامل وإنما احد تحدياتها. والخيار الأخير الذي نتبناه إصدار تشريع خاص بالتجارة والأعمال الإليكترونية ينظم من بين ما ينظم مفهوم الرسائل الإليكترونية والتواقيع الإليكترونية وغيرها، وهذا الخيار أو المسلك هو ما تتجه إليه مختلف النظم القانونية القائمة في تعاملها مع تحديات التجارة الإليكترونية.

المبحث السابع

تحديات الإثبات الإليكتروني في ميدان الأعمال المصرفية

لو تأملنا في قوانين البنوك في الدول العربية نجدها تقرر جملة أحكام تتعلق بما واجهته المصارف من مشكلات خلال عمليات التقاضي، ويُسجل في هذا الميدان جهد مميز لجمعية البنوك في الأردن في النظام الأردني في تبين هذه المشكلات وعقد عدد من الندوات العلمية النقاش حولها كما يُسجل لها دورها المميز في إيجاد هذه المادة، وفي هذا الإطار فإن هذه المادة تنشئ أحكام جديدة أو تُعدل أحكاماً قائمة في حقول نظام الإثبات والتوثيق العينية، وحوالة الحق والشيكات. وحيث أن المقام محصور بالبحث في الإثبات فإننا نتناول تالياً أحكام هذه المادة بهذا الخصوص أما ما ورد في الفقرات (أ، و، ز) فإنها موضوعات تتطلب دراسات مستقلة، ولا نُشير هنا إلى هذه الفقرات إلا في حدود اتصالها بالإثبات، ونكتفي في هذا المقام بعرض الأحكام العامة المستحدَثة وبعض تحدياتها على أن تكون محلاً للدراسة التفصيلية الخاصة من ناحية المشكلات العملية المثارة بشأنها. وأول ما يتعين لإشارة إليه، أن النص المستحدَث في قانون البنوك بشان الإثبات لا يمكن أن يسري بأثر رجعي على ما سبقه من حالات أو دعاوى، ذلك أن القانون يسري بأثر فوري وللحالات المستقبلية ما لم ينص صراحة على غير ذلك، وهو ما لم يحصل في مشروع القانون مدار البحث، كما أن القضاء الأردني مستقر على أن مسائل الإثبات محكومة بالقانون النافذ وقت التصرف أو العقد بحسب الحالة، وفي ذلك تقول محكمة التمييز الأردنية [1]:

((استقر الفقه والقضاء على أن القانون الذي يفصل في طرق الإثبات

---

(1) عرب، يونس، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، منشورات اتحاد المصارف العربية، الطبعة الأولى، 2000م.

هو القانون الذي كان معمولاً به وقت العقد حتى لو كان القانون الجديد ادخل تغييراً على ذلك. ومبنى هذه القاعدة هو أن الناس لهم حق مكتسب في أن يبقى صحيحاً بمقتضى القانون الذي كان موجوداً وقت العقد)).

أما المسألة الثانية المتعين الإشارة إليها، أن الأحكام الواردة في المادة 92 بخصوص الإثبات شأنها شأن الأحكام الواردة في طائفة التشريعات المشار إليها أعلاه، هي أحكام خاصة ينحصر قبولها وإعمال مفاعيلها على الحالات التي تطبق عليها هذه القوانين ولا تمتد إلى نزاعات أو دعاوى أخرى، لأنها أحكام خاصة تقيد القواعد العامة في الإثبات بالنسبة لما تنظمه، فالبيانات الإليكترونية حجة في حقل دعاوى الأوراق المالية سنداً لنص المادة 72/ج من قانون الأوراق المالية وذات القول يرد بالنسبة للدعاوى المصرفية لكن سنداً لنص المادة 92 من مشروع قانون البنوك. وسنرى أن هذه الحقيقة تُثير إشكالاً هاماً وكبيراً، ذلك أن تحديد نطاق النزاع الذي تطبق فيه المادة المتضمنة لقاعدة خاصة ليس دائماً أمر سهل كما سنرى لدى بحث المشكلات العملية لتطبيق النصوص المتقدم الإشارة إليها.

أما عن الأحكام الجديدة المقررة في المادة 92 مدار البحث، فهي الاعتراف بحجية البيانات الإليكترونية أو البيانات الصادرة عن أجهزة الحاسب أو مراسلات أجهزة التلكس والاعتراف بحجية الميكروفيلم، أو الصور المصغرة عن البرقيات، والإشعارات، والمراسلات، والسجلات، والكشوف، وحسم الجدل حول طبيعتها بإنزالها منزلة الأصل لا باعتبارها صورة مستنسخة عن الأصل المدخَل أو المعالج بطريقة بالميكروفيش [1]، وكذلك إنزال البيانات المخزَّنة في نظم المعلومات منزلة الدفاتر التجارية والإعفاء من مسك الدفاتر والسجلات التجارية التقليدية (م 92/د)، وأخيراً اعتبار أية علاقة مع البنك تجارية ليتحقق مبدأ جواز الإثبات فيها بكافة طرق الإثبات بما فيها الوسائل

---

(1) علي، عبد الصبور عبد القوي، التنظيم القانوني التجارة الإليكترونية، مكتبة القانون والاقتصاد، الرياض 2011م.

الإليكترونية للإثبات[1].

ويُلاحظ أن الفقرة ب من المادة 92 ذكرت صراحة البيانات الإليكترونية، ومستخرجات الحاسب، ومراسلات التلكس، لكنها لم تذكر الفاكس وتسجيلات الهاتف على خلاف قانون الأوراق المالية المشار إليه فيما تقدم، وهو ما يثير التساؤل عن مدى اعتبار الفاكسات حجة في الدعاوى المصرفية؟؟ وبالرجوع إلى النص المذكور نجده قد قرر ابتداء جواز الإثبات في الدعاوى المصرفية بكافة طرق الإثبات واستخدم بعد هذا الحكم عبارة (بما فيها .. الخ) وهو ما يدفع إلى القول أن ما أورده النص ليس أكثر من أمثلة مذكورة على سبيل المثال، غير أننا نجد أن في هذه الصياغة القانونية ما يمكن أن يُثير إشكالات حقيقية في الواقع العملي بشأن تطبيق هذا الحكم، ذلك أن نظامنا القانوني يقرر الحق في الإثبات بكافة طرق الإثبات في عدد من المنازعات، كالتجارية والجزائية والعمالية، ورغم ذلك فإن أحكام القضاء لم تتجه إلى قبول الأدلة التي تخرج عن نطاق البينات الستة المقررة في قانون البينات بسند من القول أن المقصود بكافة طرق الإثبات، الطرق التي أقر بها القانون ونظّمها واعترف لها بهذه الصفة وليس أي طريق لا يعرفه النظام القانوني، ومن هنا مثلاً لم يقبل القضاء في المنازعات التجارية الفاكس حجة في الإثبات في كل الحالات مع أن النزاعات التجارية جائز إثباتها بكافة طرق الإثبات، وبالتالي وحسماً لكل جدل كان يتعين أن يورد المشرّع في المادة 92 الفاكس والتسجيلات الهاتفية على نحو ما أوردها في قانون الأوراق المالية. سيما وأن الكمبيوتر ذاته يستخدم حالياً كجهاز مراسلات بل إن من المراسلات الصادرة عنه البريد الإليكتروني والفاكس بالمعنى المعروف، فرسالة الفاكس لم تعد حكراً على جهاز الفاكسميلي وترسل بواسطة برمجيات الفاكس المخزّنة داخل

---

(1) عرب، يونس، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، منشورات اتحاد المصارف العربية، الطبعة الأولى، 2000م.

نظم الكمبيوتر[1]، فهل نعد مثل هذه المراسلات الصادرة عن الكمبيوتر حجة باعتبارها مستخرجات للحاسوب أم أنها ليست كذلك لأنها مدروسة بعبارة (رسالة فاكسميلي) إذا ما سرنا على ما هو مستقر قضائياً من وجوب النص صراحة على البينة التي تُعد مقبولة في الإثبات [2].

وقد تناولت المادة 92 مدار البحث ولأول مرة في القانون الأردني حجية المصغرات الفيلمية أو ما يعرف بالميكروفيلم أو بالميكروفيش، فقررت أن للبنوك الحق في أن تحتفظ بصورة مصغرة (ميكروفيلم أو غيرة من أجهزة التقنية الحديثة)) بدلاً من أصل الدفاتر، والسجلات والكشوفات، والوثائق ،والمراسلات، والبرقيات، والإشعارات، وغيرها من الأوراق المتصلة بأعمالها المالية، وتكون لهذه الصورة المصغَّرة حجية الأصل في الإثبات.

والمصغَّرات الفيلمية بأشكالها المختلفة تقوم على فكرة إدخال المحرر أو الورقة الأصلية إلى أجهزة تستنسخ عنها صورة وتُخزِّنها بشكل مصغَّر أو مضغوط يُتيح استرجاعها وإعادة طباعة نسخة عنها، وتقنياً فإن المخزن في الذاكرة الإليكترونية هو صورة عن الأصل والمستخرَج من الجهاز التقني صورة عن الأصل أيضاً، وقد تم اللجوء مبكراً إلى هذه الوسائل للخلاص من أطنان الأوراق المتجمِّعة لدى البنوك، وتطورت فكرة إدخال صورة المستند إلى أنماط جديدة من القراءة الضوئية باستخدام الماسحات الضوئية وبرمجيات ضغط الملفات والوثائق والنصوص [3].

ويتعيَّن في هذا المقام تثبيت الحقائق التالية بشأن هذا النص، أولها أن النص من حيث الأصل حسم الجدل حول ما إذا كانت الحجية في الإثبات لازمة

---

(1) عرب، يونس، جرائم الكمبيوتر والانترنت، موسوعة القانون وتقنية المعلومات، منشورات اتحاد المصارف العربية، الطبعة الأولى، الجزء الثاني، 2002م.

(2) عرب، يونس، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، المرجع السابق.

(3) عرب، يونس، جرائم الكمبيوتر والانترنت، موسوعة القانون وتقنية المعلومات، الجزء الثاني، المرجع السابق.

لأصل المصغَّر الفيلمي أم للمصغَّر الفيلمي نفسه، وذلك لجهة منح الحجية للمصغَّر الفيلمي باعتباره حكماً كالأصل، لكن هذا لا يمنع أن يُثار النزاع واقعاً بشأن صور المستندات المعالجة بهذه الطريقة، وذلك بالنسبة لحالات إنكار التوقيع، أو حالات التزوير، أو نحوه، وفي كل ما يتطلب عمليات المضاهاة، وهو ما كان يتمين معه إقرار صلاحية المصغر الفيلمي للمضاهاة عند النزاع، مع أن الإشكال يبقى قائماً من حيث مدى صلاحية المصغَّر الفيلمي لعمليات المضاهاة من الوجهة التقنية كما سنرى لدى التعرُّض للمشكلات العملية المتصلة بتطبيق النص. كما أن تقديم المصغَّر الفيلمي كبينة يواجهه مشكلة تثبت القضاء من أن ما قدم له فعلاً هو مستخرج من نظام المعالجة العائد للبنك وأنه حقيقة مخزَّن فيه وهو ما قد يستدعي إصدار شهادة من البنك بذلك لتعود من جديد إلى مشكلة وجوب إبراز هذه الشهادة من منظمها، وكأننا استبدلنا إشكالات حفظ الأوراق بإشكالات الشهود على صحة الحفظ وسلامته، مع أن الإشكالات الأخيرة تظل أقل ضرراً وإعاقة من مشكلات حفظ الأوراق [1].

أما الحقيقة الثانية فهي أن قبول هذا الدليل منوط حقيقة بثقة القضاء به، وهو ما كان يستوجب - شأنه شأن مستخرجات الحاسب والبيانات الإليكترونية - أن يترافق مع اعتماد معايير تقنية موحدة لدى سائر البنوك واعتماد مواصفات نظامية تُعزز الثقة بأمن نظم المعلومات وعدم إمكان العبث ببياناتها وتحويرها، وهذه المسألة كانت محل اهتمام النظم القانونية المقارنة، إذ تلاقى إقرار حجية البيانات المحسوبة والمنقولة إليكترونياً باعتماد معايير تقنية ونظامية أهمها إتاحة الإشراف والرقابة على سلامة النظم التقنية لدى البنوك وأمنها من قبل جهات الإشراف، وهذا موضوع متشعِّب ويُثير مسائل عديدة نجد من المناسب تركه لدراسة تفصيلية مستقلة مكتفين بالقول أن احد أهم عوامل قبول أي دليل في الإثبات ثقة المتعاملين معه والقضاء

(1) علي، عبد الصبور عبد القوي، التنظيم القانوني التجارة الإليكترونية، المرجع السابق.

بصحته وسلامته إلى مدى يكفل عدم إمكان العبث به أو تحويره وهو ما يعرف بمبدأ الموثوقية والصلاحية في الاحتجاج [1].

وتُثير المادة 92 تساؤلا هاما حول مدى حق الخصوم في الدعاوى المصرفية تقديم بيانات لها نفس الطبيعة التي قبلها القانون من البنك، وبتدقيق النص نجد أن قبول البينات الإليكترونية والتلكس ومستخرجات الحاسوب جاء مطلقاً بحيث يُتيح للأطراف في الدعاوى المصرفية الاحتجاج بها، أما عن المصغَّرات الفيلمية فإن النص يُشير إلى حق البنك في الاحتفاظ بمثل هذه المصغَّرات مما يجعلها واقعاً من البيانات التي يستخدمها البنك فقط ما لم يطلبها الخصم عبر مؤسسة إلزام الخصم بتقديم بينة تحت يده[2].

(1) بيومي، حجازي عبد الفتاح، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دراسة متعمقة في جرائم الحاسب الآلي والانترنت، دار الكتب القانونية، القاهرة، 2002م.

(2) عرب، يونس، جرائم الكمبيوتر والانترنت، المركز العربي للدراسات والبحوث الجنائية، أبو ظبي 10-2002/2/12م.

المبحث الثامن

المشكلات العملية في الإثبات المصرفي بالوسائل المعلوماتية

في لقاء مجموعة الخبراء الأوروبيين القانونيين المناط بهم وضع التصور للدليل الإرشادي حول حجية سجلات الكمبيوتر والرسائل المعلوماتية المنعقد عام 1997م قيل أن الحلول الإليكترونية في بيئة العمل المصرفي لا يتعين أن تكون عبئاً إضافياً للحلول الورقية القائمة، ولتوضيح الفكرة، فإن اعتماد العمل المصرفي على التقنيات الحديثة المتعددة المحتوى والأداء والغرض، لا يجب أن يكون بحال من الأحوال وسيلة مضافة للأنماط التقليدية للعمل تسير معها لنكون في الحقيقة أمام آليتين لإدارة العمل وتوثيقه، إحداها تعتمد التقنية بما تتميز به من سرعة في الأداء وكفاءة في المخرجات وربما تكاليف أقل، وثانيها استمرار الاعتماد على الورق وعلى وسائل العمل التقليدية غير المؤتمتة، ليبقى مخزون الورق هو المخزون الاستراتيجي للعمليات المصرفية تنفيذاً وإثباتاً وتقييماً[1].

المطلب الأوّل

مشكلات المراسلات الإليكتروني

إن تحقيق درجة قبول مميزة لوسائل التعاقد والإثبات الرقمي، يتطلب برنامجاً توعوياً شاملاً، للمتعاملين ومؤسسات الأعمال والجهات القضائية والقانونية، ليس فقط للدفع نحو قبول وسائل التعاقد الإليكتروني، ولكن لإيجاد

(1) بيومي، حجازي عبد الفتاح، صراع الكمبيوتر والانترنت، في القانون العربي النموذجي، دار الكتب القانونية، القاهرة، 2007م.

ثقافة عامة تمثل الأساس للتعاطي مع كافة إفرازات عصر المعلومات الآخذة بالتطور السريع، هذه الافرازات التي تقدم يوماً بعد يوم نماذج جديدة للعمل والأداء وتتطلب توظيفاً للمنتج منها المتوائم مع مستويات الثقافة والمقبولية ومتطلبات حسن إدارة العمل. وحتى لا تكون ثمة فجوة بين قدرة المتعاملين مع التقنية وبين الجديد من فتوحها، ولضمان سلامة توظيف التكنولوجيات المستجدَة لا بد من أساس ثقافي عام يجد محتواه من خلال ترويج المعرفة بالتقنية ومتطلبات عصر المعلومات، ابتداءً من المفاهيم الأساسية ومروراً بتعظيم الفوائد والإيجابيات وتجاوز السلبيات والمعيقات، وانتهاءً بالقدرة على متابعة كل جديد والإفادة منه والتعامل معه لكفاءة واقتدار [1].

وإن نظم التقنية المؤهلة لبناء الثقة بالوسائل الإليكترونية الحديث للتعاقد والإثبات في الحقل المصرفي أو في غيره من حقول النشاط التجاري والمالي، هي النظم بسيطة البناء، المحصنة من الاعتداء على المحتوى المعلوماتي سواء من داخل المنشاة أو خارجها، المنسجمة من حيث طريقة الأداء والمخرجات مع المستقر والسائد من معايير ومواصفات تقنية، المؤهلة للاستمرار في العمل دائماً دون انقطاع أو خلل، القائمة على افتراض حصول الخلل والحاجة للبدائل الطارئة لتسيير العمل [2].

وإذا كان ثمة اهتمام لدى المؤسسات المالية بحداثة النظم ودقتها وكفاءتها من حيث السرعة وسمات التخزين، فإن الاهتمام بأمن النظم وأمن المعلومات لا يسير بالقدر ذاته، ربما لما يشهده قطاع أمن المعلومات من تطور بالغ وتغيرات متتالية ليس في الوسائل المعتمدة لتوفير أمن المعلومات فحسب بل بالنظريات التي يرتكز عليها أمن المعلومات.

إن تجربتنا البحثية المتواضعة، والحالات العملية التي تعاملنا معها أظهرت غياب استراتيجيات شاملة ودقيقة للتعامل مع أمن نظم المعلومات

(1) علي، عبد الصبور عبد القوي، التنظيم القانوني التجارة الإليكترونية، المرجع السابق.
(2) حجازي، سهير، التهديدات الإجرامية للتجارة الإليكترونية، المرجع السابق.

والبيانات المتبادلة، إذ تنطلق كثير من خطط حماية البيانات ووسائل تبادلها من نماذج مستوردة قد لا تراعي خصوصيات المنشاة وخصوصيات القواعد المعلوماتية فيها وخصوصيات التوظيف ومحدداته والثقافة السائدة، لهذا كانت أنجح الاستراتيجيات تلك القائمة على تطوير وسائل الأمن الداخلية المراعية للاعتبارات المذكورة، ولا نبالغ إن قلنا أن احد أهم أسباب فشل وسائل حماية نظم وأمن المعلومات حتى في المنشآت الكبرى يرجع إلى عدم إدراك الاحتياجات الواقعية للمنشأة وعدم مراعاة تباين النماذج الجاهزة مع الواقع الفعلي للمؤسسة [1].

ويرتبط بكفاءة النظم كفاءة المتعاملين معها وكفاءة مزودي الخدمات المتصلة بها داخليين كانوا أم خارجيين عن المنشأة، ومن هنا تكمن أهمية وظائف مستشاري النظم ومراقبي الأداء ووظائف مطوري النظم المناط بهم التواصل مع كل جديد والانفتاح على احتمالات الفشل والإخفاق بنفس القدر من الانفتاح على احتمالات النجاح والتميز.

المطلب الثاني

مشكلات التوثق من شخص المتعاقد

أن التوثق من شخص المتعاقد مرتكز تقنيات العمل المصرفي كافة، إذ لا أداء لأية عملية ولا مقبولية لإنفاذ أي طلب دون تحقيق ذلك، وسواء اختير الرقم السري أو التوقيع الرقمي أو التشفير، أو اختيرت وسائل إثبات الشخصية الفيزيائية، أو البيولوجية، أو الرقمية، أو نحوها، ودون الخوض في أي من هذه الوسائل أكثر نجاحاً أو كفاءة أو موثوقية، فإن الأهم تخير

(1) عرب، يونس، جرائم الكمبيوتر والانترنت، المركز العربي للدراسات والبحوث الجنائية، المرجع السابق.

وسيلة تقنية تفي بالفرض، تُحقق الارتياح في الاستخدام من طرف المتعامل ومن طرف القائمين بالعمل، وتتلاءم مع البناء القانوني السائد [1].

المطلب الثالث

مشكلات الإيجاب والقبول في العقد الإليكتروني

إن التعاقد الإليكتروني يتطلب التزام معيار قانوني معين لتحديد أحكام الإيجاب والقبول في البيئة الإليكترونية وتوقيت اعتبارهما كذلك قانوناً وتحدي المكان المعتَبر للتعاقد، وهذه مسائل على قدر كبير من الأهمية في حالة المنازعات، لأنها تتعلَّق بمدى قبول النظام القانوني لوجود التعاقد ابتداء وموقفه من إلزامية الإيجاب وما إذ كان القبول قد صدر صحيحاً أم لا، إلى جانب تحديد القانون المطبَّق على النزاع والمحكمة المختصة بنظره تبعاً لعناصر التنازع الزماني والمكاني. إن التعاقد الإليكتروني ومسائل الإيجاب والقبول، ومعايير اعتبارها في حقل المراسلات الإليكترونية والعقود على الخط والعقود النموذجية غير الموقعة كرخص البرامج وغيرها، أكثر مسائل البحث القانوني إثارة للجدل خلال العشرة أعوام الأخيرة لدى الهيئات والمنظمات الدولية والإقليمية الساعية لتنظيم الأعمال الإليكترونية، والتوجه العام الذي عكسه القانون النموذجي لمنظمة اليونسترال (الأمم المتحدة) ليس إلا قاعدة عريضة يُبنى عليها التدبير القانوني المناسب للنظام القانوني المعني، هذه القاعدة تقوم على أساس إحداث تساوٍ في القيمة بين العقود التقليدية والعقود الإليكترونية، بين وسائل الإثبات المؤسسة على الكتابة والتوقيع المادي وبين المراسلات الإليكترونية والتواقيع الرقمية، لكن هذه القاعدة لم تمنع الكثير

---

(1) بيومي، حجازي عبد الفتاح، صراع الكمبيوتر والانترنت، في القانون العربي النموذجي، المرجع السابق.

من الخلافات والتناقض، ولأن المقام ليس استعراض الاتجاهات الدولية، وإنما التأكيد على أن بيئة التعاقدات والأعمال الإليكترونية - ويرتبط بها مسائل الإثبات بالرسائل والوسائط الإليكترونية - لا يمكن أن تتحقق دون توفر معايير قانونية واضحة وجلية وإلى أن يتحقق ذلك تظهر الأهمية الكبيرة لبناء الوثائق العقدية للأعمال المصرفية، إذ يتعين أن تراعي هذه الوثائق غياب المعايير فتتحول بذاتها إلى قانون المتعاقدين وأن تراعي عناصر أساسية تتجاوز المشكلة أهمها تحديد القانون المطبق وجهة الاختصاص القضائي. وتركز ضمن أهم ما يتعين أن تُركز عليه على التوجه نحو طرق التقاضي البديلة التي تُجيز التحرر من كثير من القيود القانونية القائمة، ولعل التحكيم والمفاوضات والوساطة وغيرها من طرق فض المنازعات خارج المحاكم الأنسب للنشاط المصرفي وتعدو ضرورية للأعمال المتصلة بالعلاقات القانونية في البيئة الإليكترونية والمعلوماتية [1].

المطلب الرابع

مشكلات حجية الوسائل المعلوماتية في الإثبات والإقرار بها

ثمة اتجاه دولي عريض نحو الاعتراف بحجية المراسلات الإليكترونية بمختلف أنواعها والاعتراف بحجية الملفات المخزَّنة في النظم ومستخرجات الحاسب والبيانات المسترجَعة من نظم الميكروفيلم والميكروفيش، وحجية الملفات ذات المدلول التقني البحت، والإقرار بصحة التوقيع الإليكتروني وتساويه في الحجة مع التوقيع الفيزيائي والتخلي شيئاً فشيئاً عن أية قيود

(1) الخليل، عماد علي، التكييف القانوني لإساءة استخدام أرقام البطاقات عبر شبكة الانترنت، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، الذي نظمته كلية الشريعة والقانون، بجامعة الإمارات العربية المتحدة، عام2000م.

تحد من الإثبات في البيئة التقنية، والسنوات القليلة القادمة ستشهد تطوراً أيضاً في الاتجاه نحو قبول الملفات الصوتية والتناظرية والملفات ذات المحتوى المرئي وغيرها [1].

واتجه المشرِّع الأردني نحو قبول الوسائل الإليكترونية كبينة في الدعاوى المصرفية، وقد عالجنا في العدد السابق موقف قانون البنوك الجديد وما قرره في هذا الصدد، ولا نكرر ما قلناه مكتفين بالإشارة إلى أن المشكلة لا تزال تكمن في التعاطي الجزئي مع تدابير عصر المعلومات التشريعية، ومع التأكيد على تفهُّمنا للواقع وتقديرنا العالي لما ينجز إلا أن قانون البينات وأحكام التعاقد المدني والتجاري تظل حجر أساس تعكس مدى تفهُّمنا لمتطلبات عصر المعلومات [2].

---

(1) بيومي، حجازي عبد الفتاح، صراع الكمبيوتر والانترنت، في القانون العربي النموذجي، المرجع السابق.

(2) علي، عبد الصبور عبد القوي، التنظيم القانوني التجارة الإليكترونية، المرجع السابق.

المبحث التاسع

الأدلة المعلوماتية في المواد الجنائية

مع ازدياد الاعتماد على نظم الكمبيوتر والشبكات في الأعمال أُثيرت ولا تزال تثار مشكلة أمن المعلومات، أي حماية محتواها من أنشطة الاعتداء عليها، سواء من داخل المنشاة أو من خارجها، وأنماط الاعتداء عديدة تبدأ من الدخول غير المصرَّح به لملفات البيانات إلى إحداث تغيير فيها وتحوير بمحتواها أو صُنع بيانات وملفات وهمية، أو اعتراضها أثناء نقلها، أو تعطيل عمل النظام، أو الاستيلاء على البيانات لأغراض مختلفة أو إحداث تدمير أو احتيال للحصول على منافع ومكاسب مادية أو لمجرد الإضرار بالآخرين وحتى لإثبات القدرة وأحياناً مجرد أنشطة تستهدف المزاح الذي سرعان ما يكون عملاً مؤذياً يتجاوز المزاح [1].

المطلب الأوّل

الطبيعة الخاصة بالأدلة في جرائم المعلوماتية

القاعدة العامة في الدعاوى الجزائية جواز الإثبات بكافة طرق الإثبات القانونية، والقيد على هذه القاعدة أن الدليل يتعين أن يكون من الأدلة التي يقبلها القانون، وبالتالي تظهر أهمية اعتراف القانون بالأدلة ذات الطبيعة الإليكترونية، خاصة مع احتمال ظهور أنشطة إجرامية عديدة في بيئة الأعمال والتجارة والبنوك الإليكترونية.

---

(1) بيومي، حجازي عبد الفتاح، صراع الكمبيوتر والانترنت، في القانون العربي النموذجي، المرجع السابق.

والمعلومات، وإن كانت قيمتها تتجاوز شيئاً فشيئاً الموجودات والطاقة، فإنها ليست ماديات لتقبل بينة في الإثبات، ووسائط تخزينها غير الورق كمخرجات لا تحظى بقبولها دليلاً مادياً، من هنا كان البحث القانوني في العديد من الدول يتجه إلى الاعتراف بالحجية القانونية لملفات الكمبيوتر ومستخرجاته والرسائل الإليكترونية ذات المحتوى المعلوماتي ليس بصورتها الموضوعة ضمن وعاء مادي ولكن بطبيعتها الإليكترونية المحضة (1).

فالمشكلة تكمن في القواعد المخُزنة، في صفحات الفضاء الإليكتروني، في الوثيقة الإليكترونية إذ ما تحتويه من بيانات قد يكون الدليل على حصول تحريف أو دخول غير مصرَّح به أو تلاعب، فكيف يقبلها القضاء وهي ليست دليلاً مادياً يُضاف إلى الملف كمحضر أقوال الشاهد مثلاً أو تقرير الخبرة، ولتجاوز هذه المشكلة يلجأ القضاء إلى انتداب الخبراء لإجراء عمليات الكشف والتثبّت من محتوى الوثائق الإليكترونية ومن ثم تقديم التقرير الذي يُعد هو البينة والدليل وليس الوثائق الإليكترونية، لكنه مسلك تأباه بعض النظم القانونية عوضاً عن معارضته لأسس وأغراض إجراء الخبرة وطبيعتها كبينة تخضع للمناقشة والاعتراض والرفض والقبول (2).

ولقد اتجه الاتحاد الأوروبي منذ منتصف الثمانينات إلى توجيه مشرِّعي دول أوروبا لإقرار حجية الوثائق الإليكترونية ومساواتها بالوثائق الكتابية من حيث الحكم، والأهم من ذلك التوجيه بعدم اشتراط أن تبرز من قبل منظميها والاستعاضة عن ذلك بشهادات خطية صادرة عن الجهات مالكة النظم أو جهات وسيطة، لما ظهر عملياً من مشكلات أبرزها أن جانباً من المعلومات لا يدخلها أو يُنظمها الأشخاص وإنما يخلقها الجهاز نفسه ضمن عمليات المعالجة وفي إطار تقنيات البرمجيات القائمة على الذكاء الصناعي.

---

(1) الجنيبهي، منير، والجنيبهي، ممدوح، صراخ الانترنت وسائل مكافحتها، 2005 م، دار الفكر الجامعي، الإسكندرية .

(2) حجازي، سهير، التهديدات الإجرامية للتجارة الإليكترونية، المرجع السابق.

المطلب الثاني

الخصوصية والقواعد العامة وضمانات المتهم المعلوماتي

البيانات المخزّنة داخل النظم ليست جميعاً تتصل بجريمة الاعتداء على النظام، منها بيانات خاصة وأخرى ذات قيمة استراتيجية؛ لهذا اهتم الخبراء القانونيون بمخاطر الاعتداء على الخصوصية أو الحياة الخاصة في معرض الكشف عن الدليل أو في معرض الإقرار باستخدام دليل ذي طبيعة إليكترونية، وفي أي دولة ليس ثمة بعد قواعد لحماية الخصوصية سواء من حيث تنظيم أعمال جمع وتخزين ومعالجة ونقل البيانات، أو من حيث حقوق الدخول إليها وحق أصحابها بسلامتها وصحتها وتعديلها، أو من حيث إقرار الحمايات الإدارية التنظيمية والمدنية والجزائية لهذه البيانات، يكون ثمة صعوبة في حماية الخصوصية ويكون ثمة احتمالات كبيرة لإهدار الأدلة غير القانونية ونشوء نزاعات في هذا الحقل [1].

إن النظم القانونية المقارنة وفي الوقت الذي تحركت فيه نحو حماية المعلومات وإقرار حجية الأدلة ذات الطبيعة التقنية اتجهت أيضا من زاوية أخرى لإقرار ضمانات دستورية للمتهم المعلوماتي وضمانات إجرائية لكفالة سلامة اجراءات الملاحقة الجزائية في الدعاوى المتصلة بالمعلومات ونظم الكمبيوتر. أبرزها الحق بالخبرة المقابلة للخبرة المجراة من النيابة، والحق بعدم إجراء أية عمليات ضبط وتفتيش على نظم الكمبيوتر دون حضور المعني أو مَن يُمثله قانوناً، وإذا كانت الخصوصية وسرية البيانات أمر ذو أهمية

---

(1) عرب، يونس، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، المرجع السابق.

بالغة في شتى المواقع والقطاعات فإنها تكتسي أهمية أوسع في القطاع المصرفي، مرد ذلك التزام البنك القانوني بالحفاظ على السرية واحترام الخصوصية وتحمله مسئوليات الإفشاء بالسر المصرفي [1].

المطلب الثالث

مشكلات التفتيش والضبط

إن تفتيش مسرح الجريمة وما يتصل به من أماكن وضبط المحرزات ذات العلاقة بالجرم أمور نظمتها قوانين الأصول، ويثور التساؤل حول مدى انطباق القواعد القائمة على حالة تفتيش نظم الكمبيوتر وقواعد البيانات، ليس ذلك فحسب، بل تُثير أهمية الخبرة في هذا الحقل إذ كما يرى أحد أشهر محققي التحقيقات الفيدرالية الأمريكية أن الخطأ في تفتيش وضبط الدليل قد يؤدي إلى فوات فرصة كشف الجريمة أو فوات فرصة الإدانة حتى مع معرفة الجاني، إن تفتيش نظم الحاسبات تفتيش للفضاء الافتراضي وأوعية التخزين، تفتيش للإجراءات التي يحفظها الجهاز إن كان مزوداً بحافظات إليكترونية للعمليات المنجَزة عبره، وهو أمر يتعلق بالقدرة على تحديد المطلوب مسبقاً وليس مجرد سبر غور نظام إليكتروني، لأن التعامل وفق المسلك الأخير قد يكون له عواقب قانونية أهمها بطلان الإجراءات لأنها خارج نطاق أمر التفتيش والضبط أو قد تنطوي الإجراءات على كشف خصوصية البيانات المخزنة في النظام[2].

---

(1) علي، عبد الصبور عبد القوي، التنظيم القانوني التجارة الإليكترونية، المرجع السابق.

(2) قايد، أسامة عبد الله، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، 1994م.

المبحث العاشر

وسائل فض منازعات التجارة الإليكترونية

تؤكد المؤتمرات الدولية في هذا الحقل على أهمية الوسائل البديلة لفض المنازعات ADR وعلى تمتعها بسمات فاعلة لمواجهة منازعات التجارة الإليكترونية والملكية الفكرية، باعتبارها تُساهم في حل مشكلة الاختصاص والقانون الواجب التطبيق، وتختصر الوقت والكلفة وتحمي السمعة على نحو يتفق مع مشروعات تقنية المعلومات، وتؤكد المؤتمرات الدولية أيضاً على تشجيع إيراد شروط اللجوء للتحكيم، أو الوساطة، أو المفاوضات كبديل للقضاء ضمن تعاقدات التجارة الإليكترونية، وفي هذا الحقل تبرز تجارب عالمية وعربية مميزة، كتجربة مركز تحكيم الوايبو (منظمة الملكية الفكرية) وتجربة الاتحاد الأوروبي في وضع استراتيجيات وأدلة توجيهية لتسوية المنازعات خارج المحاكم وإدخال الوسائل الإليكترونية لتسوية المنازعات، وفي البيئة العربية ثمة تجارب مميزة يجري تطويرها وتعزيز دورها، وخبرة المحكمين المختارين مراكز وطنية وإقليمية ودولية يمكن أن تساهم في تجاوز مشكلات التخصص والخبرة الفنية في مسائل تقنية المعلومات خاصة تلك المتعلقة بالمحتوى التقني للمنازعات [1].

وتجدر الإشارة إلى أحدث تطور عالمي في حقل فض المنازعات وهو العمل على حل المنازعات المتصلة بتقنية المعلومات والانترنت بشكل إليكتروني وعلى شبكة الانترنت نفسها ضمن ما يعرف بالتسويات الإليكترونية والمحاكم الإليكترونية، وثمة توجه إلى اعتماد أنظمة كمبيوتر ذكية تعتمد على قواعد

(1) عرب، يونس، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، المرجع السابق.

بيانات شاملة تُتيح تلقي عناصر النزاع وفق القانون المعني وتقديم الحل لها، وبالرغم من ممارسة أكثر من 40 جهة في العالم مثل هذا النشاط إلا أن ما ساهم في تحقيقه توفر البناء الشامل لتشريعات تقنية المعلومات [1].

(1) حجازي، سهير، التهديدات الإجرامية للتجارة الإليكترونية، المرجع السابق.



تطبيقات قضائية

إن من أكثر المسائل في حقل الأبعاد الإجرائية لدعاوى المعلوماتية في نطاقيها الحقوقي والجزائي، مسألة نطاق الإفشاء بالمعلومات المطلوبة أو الجائزة للشاهد المعلوماتي - إن جاز التعبير، فالشاهد يشهد فيما شهد بذاته أو قال أو علم، لكن الأمر في دعاوى المعلوماتية مختلف، إذ ثمة نظام معين للمنشأة وثمة أعمال لا تتصل بالشاهد بذاته، بل ربما لا تتصل بشخص طبيعي وقد تكون متصلة بنظام إليكتروني أو نحوه، كما أن الشاهد يعلم الكثير وجزء مما يعلم واقع ضمن إطار الخصوصية والسرية [1].

إن التنظيم القانوني للقواعد الإجرائية والإثباتية في الدعاوى المعتمدة على أدلة معلوماتية أو تتصل بعوالم التقنية والإليكترونيات يجب إعادة توصيفها قانوناً بل وتنظيمها بشكل لا يضع الشاهد موضع المساءلة ولا يحرم القضاء فرصة الإفادة من شهادة الشاهد في سبر غور الحقيقة التي تتوقف في أحيان كثيرة على ما يعلمه الشاهد بالخبرة النظرية لا ما يعلمه بالواقع من حقائق رآها، أو سمعها، أو نقلت له.

- أظهرت بعض الوقائع العملية أن القضاء يعتمد على نفسه أولاً وعلى

---

(1) قايد، أسامة عبد الله، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، 1994م.

خبرات فنية يقلبها بعناية للوصول إلى الحقيقة، ففي قرار صادر عن محكمة الاستئناف الأردنية (محكمة استئناف عمان في الدعوى رقم 2000/1313 تاريخ 2000/5/18م) بوصفها المرجع القضائي الأخير للطلبات المستعجلة قضى فيه ببطلان ضبط تسجيلات صوتية، قررت المحكمة إخضاع كافة المضبوط في ميدان الملكية الفكرية إلى شرائط القانون والحكم بعدم قبول أي ضبط دون خبرة قاطعة بحصول السلوك الإجرامي من الشخص المنسوب إليه الفعل بذاته، وينظر القضاء للأمر بكل عناية وموضوعية. وقد أظهرت الدعاوى المنظورة وعدد من المفصولة حتى الآن اتجاهاً قضائياً يقوم على تمحيص الحقائق إلى أبعد مدى لتبين الحقائق حول التراخيص سيما في ظل تنوعها وفي ظل ما يعلن على الملأ من إمكان الترخيص اللاحق للبرامج القائمة، بل في ظل صفقات الترخيص المسماة (التواؤم مع متطلبات القانون) فهي – ونحن لسنا ضدها على الإطلاق بل نُشجعها – تُثير من الوجهة القانونية التساؤل حول بعض الخبرات الفنية التي لا تقبل تراخيص بزعم مخالفتها لمعايير مقررة لدى جهات الترخيص التي هي الشركات الأجنبية المنتجة ذاتها، كالمغايرة بين رقم الرخصة والبرنامج مع أنه غير متطلب ابتداءً، والأساس – كما ذكرنا – التطابق بين الرخصة ونوع البرنامج وتاريخ تنزيله، فجهات الترخيص عند عقد الصفقات تكيف معاييرها لتمرير صفقاتها التجارية، لكنها في ساحات القضاء قد تتمسك بمعاييرها هي لضمان مركز أفضل أمام القضاء. ومن هنا فإن كافة الخبراء الفنيين العرب مدعوون للتعامل الدقيق والحذر مع الحالات المكلفين بها، لأن العلم لا يقبل التطويع لحساب سياسات نفعية، والقضاء يبذل كل جهد للوصول إلى الحقائق الموضوعية، ولأن كثيراً من المفاهيم تغيب في أوقات يفترض أن لا تغيب، وكثير مما يعتقد أنه حقيقة علمية لا يعدو مجرد سياسة تسويقية لشركة مستفيدة أو منتفعة.

– محكمة الاستئناف الأردنية وفي أحدث أحكامها (الدعوى الاستئنافية رقم2001/207م الصادر قرارها بتاريخ 2001/2/21م) في ميدان دعاوى المسئولية عن قرصنة برامج الكمبيوتر، حللت بكل دقة وعمق النصوص

الجنائية المقررة في قانون حق المؤلف الأردني، وتوصلت بوضوح إلى أن الأنشطة المجرمة في هذا الحقل تنحصر بأنشطة الاستغلال المالي المتمثلة بالعرض للبيع أو التأجير، وفي حدود غرض محدَّد فقط وهو الاستغلال الماليَ، ومن هنا قرَّرت بوضوح أن الاستخدام دون الاستغلال المالي لا يُعد جرماً وفق قانوناً، وأنهت نهاية موضوعية وعادلة واحدة من دعاوى الملكية الفكرية التي طالت واحدة من المؤسسات المالية الكبرى، ولا نبالغ إن قلنا أن حماية الإبداع بكل صوره في ميدان الملكية الأدبية والصناعية قام على أساس الموازنة بين احتياجات المبدع لصيانة إبداعه ومنحه الفرصة (المؤقتة بمدة معينة) لاستثمار نتاج عقله، وبين حاجة المجتمع للمعرفة ووسائلها، هذه الموازنة التي تمنع احتكار صاحب المصنَّف لمصنفه وتُجيز ترخيصه إجبارياً لحماية الثقافة وتلبية احتياجات التنمية والتطور في المجتمع. وإذا كان من حق مالك حقوق أي مصنِّف أن يحمي إبداعه، فإن من حق مجتمعنا علينا أن لا تكون هذه الحماية على نحو يمس عناصر تطوره ويخل بميزان التناسب بين الحماية الخاصة والاحتياجات الجماعية.

- أشارت أحد التقارير إلى أن هواة إرسال البريد المزعج أو ما يُطلق عليهم spammers يقومون بإنشاء مواقع لاختصار الروابط خاصة بهم، في محاولة جديدة لمراوغة والتحايل على مبادرات مكافحة البريد المزعج على الانترنت.

وقد رصدت شركة سيمانتك للحماية هذه المواقع لأول مرة في أبريل/ نيسان 2011م، حيث تُتيح هذه المواقع لمرسلي البريد المزعج تجنُّب المرشحات التلقائية وإخفاء الحقيقة وراء روابطهم المضللة التي توجه المستخدمين إلى مواقع سيئة غير مرغوب فيها.

على سبيل المثال إذا أراد أحد القراصنة استدراج الضحايا لأحد المواقع الموجودة في القائمة السوداء في مواقع اختصار الروابط الشرعية مثل موقع خاص بالمخدرات، إذ يقوم باختصار الرابط في أحد مواقع اختصار الروابط

غير الشرعية ثم إرسال الرابط المستتر لأحد مواقع الاختصار الشرعية ليتم اختصاره مرة ثانية.

ثم يتم استخدام الرابط المختصر النهائي كطعم يتم إرساله في رسائل البريد المزعج. وإذا لم يتم اكتشافه بواسطة برامج فلترة البريد المزعج يمكن أن يقوم المستخدمين عديمي الخبرة بالنقر على هذه الروابط التي بدورها تقوم بتوجيههم إلى المواقع غير المرغوب فيها.

وتجدر الإشارة إلى أن جميع مواقع اختصار الروابط المستخدَمة من قبل القراصنة تحتوي على. ru في أسماء النطاقات الخاصة بها وكلها مستضافة في روسيا وأوكرانيا.

- أثبتت الإحصائيات إلى تصدُّر المملكة العربية السعودية المركز الأول على مستوى دول الخليج العربي في التعرُّض للجرائم الإليكترونية، وذلك وفقاً لما ذكرته شركة (تريند مايكرو) إلى وجود أكثر من 700 ألف حالة انهيار نظامي خلال تسعة شهور فقط في السعودية بنسبة 64% [1].

مما أدى إلى فقد المملكة العربية السعودية ثقتها بالتعامل الإليكتروني عبر الانترنت مما يحتم وجود قانون مكافح لمثل هذه الجرائم.

وعليه فإن مجلس الوزراء الموقَّر أقر في جلسته يوم الاثنين 7 ربيع الأول 1428هـ برئاسة خادم الحرمين الشريفين الملك عبد الله بن عبد العزيز - حفظه الله - نظام مكافحة جرائم المعلوماتية، بتحديد الجرائم والعقوبات المقررة لها للحد من نشوءها. وتتجاوز مجموع العقوبات المالية الواردة في النظام مبلغ 11 مليون ريال، موزَّعة بالتفاوت المبني على فداحة الجرم الإليكتروني المرتَّكب. فرض النظام عقوبة بالسجن مدة لا تزيد عن سنة واحدة وغرامة مالية لا تزيد على 500 ألف ريال أو بإحداهما، على

(1) المملكة العربية السعودية والإمارات في صدارة ضحايا الجرائم الإليكترونية، http://www. alarabiya. net/articles/2009/11/15/91413. html#00 (1545

كل شخص يرتكب أياً من الجرائم المنصوص عليها في نظام أمن المعلومات، وعرف القانون بعضاً من أنواع تلك الجرائم منها الدخول غير المشروع إلى موقع إليكتروني أو الدخول إلى موقع إليكتروني بهدف تغيير تصاميم هذا الموقع، أو إلغائه، أو إتلافه، أو تعديله، أو شغل عنوانه، إساءة استخدام الهواتف النقالة المزودة بكاميرا أو ما في حكمها للمساس بالحياة الخاصة للأفراد بقصد التشهير وإلحاق الضرر بهم عبر وسائل تقنيات المعلومات المختلفة، كأدنى عقوبة تذكر في النظام. وفرض النظام عقوبة بالسجن مدة لا تزيد عن عشر سنوات وبغرامة مالية لا تزيد عن خمسة ملايين ريال أو بإحداهما، على كل شخص يُنشئ موقعاً للمنظمات الإرهابية على الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي، أو نشره لتسهيل الاتصال بقيادات تلك المنظمات أو ترويج أفكارها، أو نشر كيفية صنع المتفجرات وما يتم استخدامه في الأعمال الإرهابية، كأقصى عقوبة تذكر في النظام.

وتطبيقاً لذلك ظهر أول حكم قضائي لجريمة إليكترونية في المملكة والذي صدر من المحكمة الجزئية في الإحساء، حيث تم الحكم على شاب سعودي بالسجن 21 شهراً والجلد 200 جلدة بالإضافة لغرامة مالية قدرها 50 ألف ريال جراء قيامه باختراق البريد الإليكتروني لفتاة سعودية والاستيلاء على صورها الخاصة الموجودة به، وتهديدها بنشر صورها إذا لم تستجب لمطالبه، وكان ذلك نتيجة قيام الفتاة برفع دعوى ضد الشاب انتهت بصدور هذا الحكم[1].

– وجوب اشتماله على بيان الواقعة المستوجبة للعقوبة والظروف التي وقعت فيها والأدلة التي استخلصت منها المحكمة ثبوت وقوعها من المتهم. المادة 310 إجراءات. جريمة النصب المنصوص عليها بالمادة 336 عقوبات. مناط تحققها. الطرق الاحتيالية في جريمة النصب. ما يلزم لتوافرها. إدانة الطاعن

---

(1) من الرابط http://coeia. edu. sa/index. php/ar/asurance-awarness/articles/43-malware-attacks-n-threats/1177-cyber-crime-laws-in-saudi-arabia. html

في جريمة النصب. استناداً إلى محضر الضبط دون بيان مضمونه والطرق الاحتيالية التي استخدمها والصلة بينها وبين تسليم المجني عليه المال موضوع الإتهام. قصور القاعدة: لما كانت المادة 310 من قانون الإجراءات الجنائية قد أوجبت في كل حكم بالإدانة أن يشتمل على بيان الواقعة المستوجبة للعقوبة بياناً تتحقق به أركان الجريمة التي دان المتهم بها والظروف التي وقعت فيها والأدلة التي استخلصت منها المحكمة ثبوت وقوعها من المتهم وكانت جريمة النصب كما هي معرفة في المادة 336 من قانون العقوبات تتطلب لتوافرها أن يكون ثمة احتيال وقع من المتهم على المجني عليه بقصد خداعه والاستيلاء على ماله، فيقع المجني عليه ضحية الاحتيال الذى يتوافر باستعمال طرق احتيالية، أو باتخاذ اسم كاذب، أو بانتحال صفة غير صحيحة، أو بالتصرف في مال الغير ممن لا يملك التصرف فيه، وقد نص القانون على أن الطرق الاحتيالية في جريمة النصب يجب أن يكون من شأنها الإيهام بوجود مشروع كاذب، أو واقعة مزورة، أو إحداث الأمل بحصول ربح وهمي أو غير ذلك من الأمور المبينة على سبيل الحصر في المادة 336 من قانون العقوبات المشار إليها لما كان ذلك وكان الحكم المطعون فيه قد تساند في إدانة الطاعن إلى محضر الضبط دون أن يُبين مضمونه وما إستدل به على ثبوت التهمة في حق الطاعن، والطرق الاحتيالية التي استخدمها، والصلة بينها وبين تسليم المجني عليه المال موضوع الاتهام، فإنه يكون مشوباً بالقصور في بيان الواقعة واستظهار أركان جريمة النصب التي دان الطاعن بها - الأمر الذى يعجز محكمة النقض عن إعمال رقابتها على تطبيق القانون تطبيقاً صحيحاً على واقعة الدعوى كما صار إثباتها في الحكم مما يتعين معه نقض الحكم. (المادتان 336 من قانون العقوبات، 310 من قانون الإجراءات الجنائية).

- جريمة النصب بالاستعانة بشخص آخر. شرط وقوعها مثال لحكم بالبراءة في جريمة نصب. صادر من محكمة النقض لدى نظرها موضوع إتيان القاعدة: من المقرر أن يشترط لوقوع جريمة النصب بطريق الاستعانة ص146). على تأييد الأقوال والادعاءات المكذوبة، أن يكون الشخص الآخر

قد تداخل بسعي من الجاني وتدبيره وإرادته لا من تلقاء نفسه بغير طلب أو اتفاق، وأن يكون تأييد الآخر في الظاهر لادعاءات الفاعل تأييداً صادرا عن شخصه هو لا مجرد ترديد لأكاذيب الفاعل لما كان ذلك، وكان البين من وقائع الدعوي أن المتهم لم يكن هو الذي سعى إلى المجني عليه كي يعرض عليه قطعة الأرض محل التعامل بينهما، بل على العكس من ذلك، فان المدَّعي بالحقوق المدنية هو الذى توجه إلى المتهم في محله طالباً منه بيعه الأرض على حد قوله ولم ينسب له إتيان أي فعل مما يُعد من وسائل الاحتيال، فقد اقتصر الأمر على اتفاقهما على التعامل شفاهة وسلم المدَّعي بالحقوق المدنية الشيكات للمتهم، هذا إلى أن أقوال المدَّعي بالحقوق المدنية لا تكشف عن قيام بتأييد أقوال المتهم بشأن الأرض أو أنه أرشده عن المتهم بسعي ...... من الأخير أو تدبيره، مما تخرج به الواقعة برمتها عن نطاق التأثيم، ويتعين القضاء ببراءة المتهم. (م 336 عقوبات) (الطعن رقم 8996 لسنة 58 ق جلسة 17/1/1990 س 41 ص146).

- هذه الحادثة هي أحد أول الهجمات الكبيرة والخطرة في بيئة الشبكات ففي تشرين الثاني عام 1988م تمكن طالب يبلغ من العمل 23 عاماً ويدعى ROBER MORRIS من إطلاق فيروس عرف باسم (دودة موررس) عبر الانترنت، أدى إلى إصابة 6 آلاف جهاز يرتبط معها حوالي 60000 نظام عبر الانترنت من ضمنها أجهزة العديد من المؤسسات والدوائر الحكومية، وقد قدرت الخسائر لإعادة تصليح الأنظمة وتشغيل المواقع المصابة بحوالي مائة مليون دولار إضافة إلى مبالغ أكثر من ذلك تمثل الخسائر غير المباشرة الناجمة عن تعطل هذه الأنظمة، وقد حكم على مورس بالسجن لمدة 3 أعوام وعشرة آلاف غرامة.

- وفي حادثة هامة أخرى، انخرطت جهات تطبيق القانون وتنفيذه في العديد من الدول في تحقيق واسع حول إطلاق فيروس شرير عبر الانترنت عرف باسم فيروس MELISSA حيث تم التمكن من اعتقال مبرمج كمبيوتر من ولاية نيوجرسي في شهر نيسان عام 1999 م واتهم باختراق اتصالات عامة

والتآمر لسرقة خدمات الكمبيوتر، وتصل العقوبات في الاتهامات الموجهة له إلى السجن لمدة 40 عام والغرامة التي تقدر بحوالي 500 الف دولار وقد صدر في هذه القضية مذكرات اعتقال وتفتيش بلغ عددها 19 مذكرة.

- مصمم ومبرمج شبكات كمبيوتر ورئيس سابق لشركة omega من مدينة Delaware ويدعى Timothy Allen Lioyd (35 عاما) تم اعتقاله في 1998/2/17 بسبب إطلاقه قنبلة إليكترونية في عام 1996 م bomb بعد 20 يوماً من فصله من العمل استطاعت أن تلغي كافة التصاميم وبرامج الإنتاج لأحد كبرى مصانع التقنية العالية في نيوجرسي والمرتبطة والمؤثرة على نظم تحكم مستخدمة في nasa والبحرية الأمريكية، ملحقاً خسائر بلغت 10 مليون دولار وتعتبر هذه الحادثة مثالاً حياً على مخاطر جرائم التخريب في بيئة الكمبيوتر بل إعتبرت أنها أكثر جرائم تخريب الكمبيوتر خطورة منذ هذه الظاهرة.

- في مطلع شهر تشرين الثاني من العام 1999م، أصدر قاضي التحقيق في بيروت قراراً ظنياً في قضية سرقة اسطوانات حاسب آلي تحوي قيود السجل العقاري لدى المديرية العامة للشئون العقارية بهدف استثمارها والمتاجرة بها.

فأعتبر أن استنساخ المعلومات الموجودة بداخل «الهارديسك» الموجود في الحاسب الآلي في مديرية الشئون العقارية لا يعد سرقة لأنه لم يجر الاستيلاء عليه ككيان مادي.

كما أعتبر أن السرقة بمدلولها القانوني غير متوفرة لأنه لم يجر «أخذ الهارديسك»، ولم ينقل من مكانه، ولم يدخل في حيازة أحد من المدَّعى عليهم، بل أجرى استنساخ المعلومات الموجودة بداخله وهو بمكانه في الحاسب الآلي، وبالتالي لم يجر الاستيلاء عليه بصفته مالاً منقولاً بكيانه المادي، مما ينفي بالنتيجة تحقق أحد الأركان الأساسية لجرم السرقة المنصوص عنه في المادة 638 عقوبات.

استشهد القاضي المذكور بحالة تطبيقية سبق أن عرض لها قاضي التحقيق في جبل لبنان - وهي تشبه حالة تصوير المستند المذكورة أعلاه - عندما قرر عدم توفر أركان جرم السرقة بحق طلاب دخلوا إلى مدرستهم في غياب المسئولين عنها وتمكنوا من الوصول إلى غرفة الإدارة، ثم أخذوا من الخزانة أسئلة الامتحان أو نسخوها، معللاً ذلك بأن المدَّعى عليهم الطلاب أقدموا على سرقة الأسئلة عن طريق نسخها من دون أن يسرقوا الورقة المكتوب عليها تلك الأسئلة والتي وحدها لها الكيان المادي[1].

- قبل محكمة فرجينيا الغربية بالحبس لمدة 15 شهراً والبقاء تحت المراقبة السلوكية لمدة 3 سنوات بعد أن أقر بذنبه وأنه قام وبشكل متعمد باختراق كمبيوترات محمية الحق فيها ضرراً بالغاً في كل من ولايات فرجينيا واشنطن وإضافة إلى لندن في بريطانيا، وقد تضمن هجومه الاعتداء على مواقع لحلف الأطلسي إضافة إلى الاعتداء على موقع نائب رئيس الولايات المتحدة كما اعترف بأنه قد اطلع غيره من الهاكرز على الوسائل التي تساعدهم في اختراق كمبيوترات البيت الأبيض، وقد قام eric بتصميم برنامج أطلق عليه web bandit ليقوم بعملية تحديد الكمبيوترات المرتبطة بشبكة الانترنت التي تتوفر فيها نقاط ضعف تساعد على اختراقها، وباستخدام هذا البرنامج اكتشف أن الخادم الموجود في فيرجينيا والذي يستضيف مواقع حكومية واستراتيجية منها موقع نائب الرئيس يتوفر فيه نقاط ضعف تمكن من الاختراق، فقام في الفترة ما بين آب 1998 م وحتى كانون الثاني 1999 باختراق هذا النظام 4 مرات، وأثر نشاطه على العديد من المواقع الحكومية التي تعتمد على نظام وموقع USIA للمعلومات، وفي إحدى المرات تمكن من جعل آلاف الصفحات من المعلومات غير متوفرة مما أدى إلى إغلاق هذا الموقع لثمانية أيام، كما قام بالهجوم على مواقع لثمانين مؤسسة أعمال يستضيفها خادم شبكة LASER. NET في منطقة فيرجينيا والعديد من

(1) راجع الرابط www. alexalaw. com/t3909-topic

مؤسسات الأعمال في واشنطن إضافة إلى جامعة واشنطن والمجلس الأعلى للتعليم في فيرجينيا رتشموند ومزود خدمات انترنت في لندن، وكان عادة يستبدل صفحات المواقع بصفحات خاصة به تحت اسم ZYKLON أو باسم المرأة التي يحبها تحت اسم CRYSTAL.

- تعامل مكتب التحقيقات الفيدرالية مع قضية أطلق عليها اسم مجموعة الجحيم العالمي GLOBAL HELL فقد تمكنت هذه المجموعة من اختراق مواقع البيت الأبيض والشركة الفيدرالية الأمريكية والجيش الأمريكي ووزارة الداخلية الأمريكية، وقد أُدين اثنين من هذه المجموعة جراء تحقيقات الجهات الداخلية في الولايات المتحدة، وقد ظهر من التحقيقات أن هذه المجموعات تهدف إلى مجرد الاختراق أكثر من التدمير أو التقاط المعلومات الحساسة، وقد أمضى المحققون مئات الساعات في ملاحقة ومتابعة هذه المجموعة عبر الشبكة وتتبع آثار أنشطتها، وقد كلف التحقيق مبالغ طائلة لما تطلبه من وسائل معقدة في المتابعة.

- أقدم مستخدم، كان يعمل لدى شركة تتعاطى وضع البرامج المعلوماتية وبيعها من الغير، وبحكم اطلاعه على جميع برامج الشركة، إلى نسخ هذه البرامج واحتفظ بنسخ عنها في منزله، وبعد تقديم استقالته من الشركة، أقدم على عرض هذه البرامج للبيع إلى عدة زبائن بسعر زهيد، فأقامت عليه الشركة دعوى جزائية. فأدانه القاضي المنفرد الجزائي بجرمي المادتين 2+70 تقليد - علامة فارقة - و714 عقوبات مزاحمة احتيالية.

ولكن محكمة الاستئناف فسخت الحكم الابتدائي لجهة جرم تقليد العلامة الفارقة؛ لأن البرامج لم تكن مسجلة في دائرة حماية الملكية التجارية والصناعية، وذلك بصرف النظر عما إذا كانت هذه البرامج قابلة للتسجيل أم لا، وصدقته لجهة التجريم بجرم المزاحمة الاحتيالية.

- بتاريخ 2000/4/26م، تجنبت محكمة الجنايات في بيروت الخوض في نقاش الوصف القانوني لجرم «السرقة»، معتبرة أن نسخ المعلومات

العقارية المخزنة داخل «الهارديسك» يؤلف إعتداء على أثر فكري محمي، وطبقت عقوبة النسخ غير المشروع لبرنامج الحاسب الآلي المنصوص عنها في قانون حماية الملكية الأدبية والفنية [1].

ولكن محكمة الجنايات في بيروت قد خلطت في قرارها بين برنامج الحاسب الآلي الذي أدرجه قانون الملكية الأدبية والفنية في لائحة الأعمال الفكرية المشمولة بالحماية التي يقررها هذا القانون، وبين المعلومات غير المادية المدخلة والموثقة في ذاكرة الحاسب الآلي التي قد لا يستحوذ بالضرورة على هذا الوصف، وكذلك خلط بين مفهوم برامج الحاسب الآلي، ومجموعات الأعمال المعلوماتية، مما يدل على النقص في استيعاب القضاء للجوانب التقنية لهذه المؤلفات الجديدة [2].

● وكذلك واجه القضاء اللبناني قضية فيها تعرض كبير للآداب العامة والأخلاق العامة تمكن من معالجتها رغم حصولها في شبكة الانترنت بحيث تمكنت السلطات الأمنية اللبنانية بالتعاون مع الإنتربول من توقيف شخص لبناني كان يبث صوراً خلاعية للأطفال وذلك بأمر من النيابة العامة، التي أحالته إلى قاضي التحقيق في بيروت الذي ظن فيه بالمواد 531 و532 و533 عقوبات وفقا لمطالعة النيابة العامة، وأحاله أمام القاضي المنفرد الجزائي في بيروت الذي أدانه سنداً للمواد المذكورة.

ولكن محكمة الاستئناف الجزائية عادت وفسخت الحكم إذا اعتبرت أن عناصر الجرم المنصوص عنه في المادتين 531 و532 غير متوفرة بسبب عدم توفر شرط العلنية للجمهور المنصوص فيه في المادة 209 عقوبات، ولكنها أدانته سنداً للمادة 533 عقوبات فقط.

ولكننا نُخالف ما قضت به محكمة الاستئناف على اعتبار أن بث الصور والمشاهد الخلاعية عبر شبكة الانترنت عرضة للالتقاط من ملايين

---

(1) راجع الرابط www. startimes. com/f. aspx?t=7251666

(2) راجع الرابط www. alexalaw. com/t3909-topic

المشاهدين، إذ يكون شرط العلنية متوافراً [1].

وبتاريخ 2001/2/12، أدان القاضي المنفرد الجزائي في كسروان بجرم التقليد شخصاً أقدم على نقل وتقليد معلومات موضوعة على أسطوانات مرنة Floppy Disk تخص الشركة المدعية.

وبتاريخ 2001/10/11، أدان القاضي المنفرد الجزائي في المتن بموجب المادة 733 عقوبات شخصاً بسبب دخوله إلى مركز الشرطة حيث كان يعمل على الحاسب الآلي بغفلة عن أحد زملائه السابقين وإقدامه على انتزاع أجزاء مهمة منه وإخفائها في مركز العمل في أمكنة غير مرئية، مما أدى إلى تعطيل العمل في الشركة بضعة ساعات قبل العثور على الأجزاء المفقودة.

---

(1) راجع الرابط www. startimes. com/f. aspx?t=7251666

خاتمة

نهاية للسرد الذي عرضنا له في الفصول السابقة نستطيع أن نقول أن التطور السريع لشبكات الانترنت يتطلب مراجعة العلاقات القانونية التي تنشأ بين تلك الشبكات ومستخدميها مثل مؤدي الخدمة، والمستخدم الرئيسي ومصمم البرامج، وحقوق المؤلفين، والتجارة الإليكترونية، فعلى كافة المستويات والاستخدامات العامة الخاصة يقتضي الأمر وضع التشريعات المناسبة لمواكبة هذا التحول السريع. ويرى البعض أن هناك شبه فراغ تشريعي خص بالانترنت، وإن وجدت بعض النصوص المتفرقة في تشريعات مختلفة خاصة بالإعلام، والتجارة، والمنافسة، والصحافة، والعقوبات التي يمكن تطبيقها في مجال الانترنت. وكما سبق أن لاحظنا فإن أول مشكلة قانونية تواجه التعامل مع الانترنت أنه عبارة عن مجموعة من آلاف الشبكات المنتشرة في العالم أجمع. هذه الشبكات تتبادل وتتقاسم المعلومات فيما بينها. وأن الانترنت ليس له مكان أو موقع مادي، فهو شبكة ليس لها مكان محدّد. وهو الوضع الذي يظل غامضاً وغريباً ويؤدي بالتالي إلى التناقض بين التشريعات

والمشكلة الثانية هي كيفية التحقق من شخصية المستخدم وكذلك المشروعات على شبكة الانترنت في ظل غياب تنظيم هيكلي عالمي لاستخدام الانترنت. إلى جانب أن ملاحقة هؤلاء تتعارض مع حرية التعبير وعدم إمكانية

مصادرة البيانات الموجودة على الشبكة [1].

كما يجب التشديد على التعرُّف على شخصية المستخدمين، وأن نُبين لهم أنهم كما يجدون مساحة من الحرية وبالتالي يقع عليهم جانب من المسئوليات، لذلك يجب التعرُّف على شخصياتهم. والتعرُّف بالشخصية يقتضي من كل من ينشر بيانات على الجمهور ولو بصفة شخصية أن يكشف عن هويته.

وبالنسبة للمواقع المهنية يجب الإشارة إلى المسئول عن الموقع ويجب على مؤدي الخدمة إذا لزم الأمر أن يمد رجال الشرطة ببيانات عن الاتصالات والتي يجب حفظها لمدة عام. وقد تم تحديد بعض العقوبات كما تم إضافة جريمة بمسمى « إعطاء بيانات مزيفة»؛و ذلك حتى يتحقق التوازن بين حرية الأفراد وضرورة إمداد رجال الشرطة بالبيانات اللازمة لأداء عملهم. يبقى شيء هام يتعلق بعمل الشرطة وهو ضرورة وجود خلية بين الوزارات خصوصاً وأننا نواجه جرائم دولية تقع في عدة أماكن. ويكون دور هذه الخلية التنسيق بين الوزارات المختلفة وترتيب التعاون بينها بحيث تكون بمثابة قطب واحد يضم العديد من الخبراء الممثلين عن كل وزارة، يكون كل منهم على علم بالبيانات والتقنيات التي تنصهر فيها الوحدات المختصة المختلفة [2].

إن أهم الخصائص التي يتميز بها الانترنت هو التشابك، فمعظم الشبكات إما أن تقوم على المراسلات الخاصة أو على اتصالات عامة. فأنت إذا تصفحت نموذجاً خاصاً بسلعة ما على شبكة الانترنت فأنت في إطار اتصال عام، أما إذا قمت بإرسال أمر شراء هذه السلعة فأنت تدخل إطار المراسلات الخاصة.

وهناك توصيات فرنسية لمعالجة بعض المشكلات والمصاعب المتعلقة بجرائم الانترنت وعلى الأخص ما يتعلق بحفظ المعلومات المتعلقة بالتحقيقات والمساعدة القانونية السريعة لاقتفاء أثر المجرمين في نفس وقت ارتكاب

---

(1) www. chawkitabib. info/spip. php?article477

(2) www. journal. cybrarians. info/index. php?...

الجريمة عن طريق العديد من مؤدي الخدمة ومعرفة المستخدمين.

إن تطبيق هذه التوصيات مرهون بالتشريعات المحلية والالتزامات الدولية، مع الأخذ في الحسبان الحماية المناسبة لحقوق الأفراد. ويجب قدر الإمكان تطبيق هذه التوصيات بطريقة تُجنب أو تُقلل من تنازع قوانين الدول المختلفة وهو ما يُمثل غالباً العقبة الأساسية في مواجهة التعاون الدولي لأجهزة الشرطة. هذه التوصيات هي:

وضع التشريعات التي من شأنها السماح لمؤدي الخدمة الاحتفاظ بعينات من بعض البيانات التي تجذب العديد من المتعاملين، كذلك بيانات عن المشتركين للأغراض التجارية. وأن يعطي مؤدي الخدمة لكل مستخدم رقماً كودياً. وأن يؤكد القانون على حماية المعلومات، وأن يأخذ في الحسبان الأمن العام والقيم الاجتماعية الأخرى، خصوصاً حفظ البيانات الهامة لأغراض أمن الشبكات، أو التحقيقات، أو ملاحقات الشرطة خصوصاً ما يتعلّق بالانترنت والتقنيات المطورة الأخرى [1].

ولابد أن تسمح التشريعات لرجال الأمن المحليين أن يصدروا توجيهات لمؤدي الخدمة المحلية بحفظ البيانات ذات المصدر الأجنبي، وذلك بعد الموافقة السريعة، مع فحص الموضوع وفقاً لمقتضيات القانون المحلي وذلك بواسطة أمر قضائي محلي أو غيره.

تأمين الحفظ السريع للمعلومات الخاصة بالعملاء الموجودة والمتعلقة باتصال خاص، والتي تكون أُرسلت بواسطة واحد أو أكثر من مؤدي الخدمة، وكذلك الكشف السريع عن كمية كافية من المعلومات الخاصة بالعملاء لكي يسمح بالتعرُّف على مؤدي الخدمة والطريق الذي تم الاتصال بواسطته. كل ذلك بناء على تنفيذ أمر قضائي أو أي شيء آخر على المستوى المحلي بما يتفق مع القانون الداخلي.

---

(1) Meunier (C.): La loi du 28 Nov. 2000 relative a la criminalite informatique. Rev. Dr. pen. Crim. 2002, p 611.

تطوير هندسة الشبكة بما يدعم الأمن ويسمح عند اللزوم باقتفاء أثر الاستخدام غير المشروع للشبكة مع مراعاة احترام الحياة الخاصة لمستخدميها

اختم بقول الله تعالي: « ومن أظلم ممن ذكر بآيات ربه فأعرض عنها ونسي ما قدمت يداه إنا جعلنا على قلوبهم أكنة أن يفقهوه وفي آذانهم وقرا وإن تدعهم إلى الهدى فلن يهتدوا إذا أبدا».[1]

أسال الله أن يجعل هذا العمل خالصاً لوجهه وأن ينفعنا به يوم الدين.

عبد الصبور عبد القوي،،،،،

(1) سورة الكهف الآية 57.

ملاحق

الملحق رقم (1): قانون التوقيع الإليكتروني المصري رقم 15 لعام 2004.

الملحق رقم (2): نظام مكافحة جرائم المعلوماتية، الصادر بالمرسوم الملكي رقم: 17 بتاريخ 1428/3/8.



الملحق رقم (1)

قانون التوقيع الإليكتروني المصري رقم 15 لعام 2004

قانون تنظيم التوقيع الإليكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات،

باسم الشعب.

رئيس الجمهورية.

قرر مجلس الشعب القانون الآتي نصه، وقد أصدرناه:

مادة 1 - في تطبيق أحكام هذا القانون يقصد بالمصطلحات الآتية المعاني المبينة قرين كل منها:

(أ) الكتابة الإليكترونية: كل حروف أو أرقام أو رموز أو أي علامات أخرى تثبت على دعامة إليكترونية أو رقمية أو ضوئية أو أية وسيلة أخرى مشابهة وتعطي دلالة قابلة للإدراك.

(ب) المحرر الإليكتروني: رسالة تتضمن معلومات تنشأ أو تدمج، أو تخزن، أو ترسل أو تستقبل كلياً أو جزئياً بوسيلة إليكترونية أو رقمية أو ضوئية أو بأية وسيلة أخرى مشابهة.

(ج) التوقيع الإليكتروني: ما يوضع على محرر إليكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها ويكون له طابع متفرد يسمح بتحديد شخص الموّقع ويميزه عن غيره.

(د) الوسيط الإليكتروني: أداة أو أدوات أو أنظمة إنشاء التوقيع الإليكتروني.

(هـ) الموقّع: الشخص الحائز على بيانات إنشاء التوقيع ويوقع عن

نفسه أو عمن ينيبه أو يمثله قانوناً.

(و) شهادة التصديق الإليكتروني: الشهادة التي تصدر من الجهة المرخص لها بالتصديق وتثبت الارتباط بين الموقّع وبيانات إنشاء التوقيع.

(ز) الهيئة: هيئة تنمية صناعة تكنولوجيا المعلومات.

(ح) الوزارة المختصة: الوزارة المختصة بشئون الاتصالات والمعلومات.

(ط) الوزير المختص: الوزير المختص بشئون الاتصالات والمعلومات.

مادة 2 - تنشأ هيئة عامة تُسمى: «هيئة تنمية صناعة تكنولوجيا المعلومات»، تكون لها الشخصية الاعتبارية وتتبع الوزير المختص، ويكون مقرها الرئيسي محافظة الجيزة، ولها إنشاء فروع في جميع أنحاء جمهورية مصر العربية.

مادة 3 - تهدف الهيئة إلى تحقيق الأغراض الآتية:

(أ) تشجيع وتنمية صناعة تكنولوجيا المعلومات والاتصالات.

(ب) نقل التكنولوجيا المتقدمة للمعلومات وتحقيق الاستفادة منها.

(ج) زيادة فرص تصدير خدمات الاتصالات وتكنولوجيا المعلومات ومنتجاتها.

(د) الإسهام في تطوير وتنمية الجهات العاملة في مجال تكنولوجيا المعلومات والاتصالات.

(هـ) توجيه وتشجيع وتنمية الاستثمار في صناعة تكنولوجيا المعلومات والاتصالات.

(و) رعاية المصالح المشتركة لأنشطة تكنولوجيا المعلومات.

(ز) دعم البحوث والدراسات في مجال تكنولوجيا المعلومات والاتصالات وتشجيع الاستفادة بنتائجها.

(ح) تشجيع ودعم المشروعات الصغيرة والمتوسطة في مجال استخدام وتوظيف آليات المعاملات الإليكترونية.

(ط) تنظيم نشاط خدمات التوقيع الإليكتروني وغيرها من الأنشطة في مجال المعاملات الإليكترونية وصناعة تكنولوجيا المعلومات.

مادة 4 - تُباشر الهيئة الاختصاصات اللازمة لتحقيق أغراضها على الأخص ما يأتي:

(أ) إصدار وتجديد التراخيص اللازمة لمزاولة أنشطة خدمات التوقيع الإليكتروني وغيرها من الأنشطة في مجال المعاملات الإليكترونية وصناعة تكنولوجيا المعلومات، وذلك وفقاً لأحكام القوانين واللوائح المنظمة لها.

(ب) تحديد معايير منظومة التوقيع الإليكتروني بما يؤدي إلى ضبط مواصفاتها الفنية.

(ج) تلقي الشكاوى المتعلقة بأنشطة التوقيع الإليكتروني والمعاملات الإليكترونية وتكنولوجيا المعلومات واتخاذ ما يلزم في شأنها.

(د) تقييم الجهات العاملة في مجال أنشطة تكنولوجيا المعلومات وتحديد مستوياتها الفنية بحسب نتائج هذا التقييم.

(هـ) تقديم المشورة الفنية بشأن المنازعات التي تنشأ بين الأطراف المعنية بأنشطة التوقيع الإليكتروني والمعاملات الإليكترونية وتكنولوجيا المعلومات.

(و) تقديم المشورة الفنية إلى الجهات العاملة في أنشطة تكنولوجيا المعلومات، وتدريب العاملين فيها.

(ز) إقامة المعارض والمؤتمرات والندوات المتخصصة في مجال تكنولوجيا المعلومات والاتصالات داخلياً وخارجياً.

(ح) إنشاء الشركات التي تساعد في تنمية صناعة تكنولوجيا المعلومات والاتصالات أو المساهمة فيها.

(ط) إيداع وقيد وتسجيل النسخ الأصلية لبرامج الحاسب الآلي وقواعد البيانات، التي تتقدم بها الجهات أو الأفراد الناشرون والطابعون والمنتجون لها للمحافظة على حقوق الملكية الفكرية وغيرها من الحقوق.

مادة 5 - يفرض لصالح الهيئة رسم بواقع واحد في المائة من إيرادات الخدمات والأعمال التي تقدمها المنشآت العاملة في مجال تكنولوجيا المعلومات والاتصالات تلتزم به هذه المنشآت، يودع في حساب خاص للمساهمة في تنمية ص الهيئة.

كما يكون إصدار وتجديد التراخيص المنصوص عليها في البند (أ) من المادة (4) من هذا القانون بمقابل يصدر بتحديد فئاته وبقواعد وإجراءات اقتضائه قرار من مجلس إدارة الهيئة.

مادة 6 - تتكون موارد ومصادر تمويل الهيئة مما يأتي:

(أ) الاعتمادات التي تخصصها لها الدولة.

(ب) الرسم المنصوص عليه في الفقرة الأولى من المادة (5) من هذا القانون.

(ج) المقابل المنصوص عليه في الفقرة الثانية من المادة (5) البند (ج) من المادة (9)، المادتين (19)، (22) من هذا القانون.

(د) مقابل الخدمات الأخرى التي تؤديها الهيئة.

(هـ) الهبات والتبرعات والإعانات التي يقبلها مجلس إدارة الهيئة.

(و) القروض والمنح التي تعقد لصالح الهيئة.

(ز) عائد استثمار أموال الهيئة.

مادة 7 - تكون للهيئة موازنة مستقلة يجري إعدادها وفقاً لقواعد إعداد موازنات الهيئات الاقتصادية، وتبدأ السنة المالية للهيئة مع بداية السنة المالية للدولة وتنتهي بانتهائها، ويكون للهيئة حساب خاص لدى البنك المركزي المصري تودع فيه مواردها، ويجوز بموافقة وزير المالية فتح حساب للهيئة في احد البنوك.

ويُرحل الفائض من موازنة الهيئة من سنة إلى أخرى. ويجوز بقرار من رئيس مجلس الوزراء بناء على عرض الوزير المختص بعد التشاور مع وزير المالية أن يؤول جزء من الفائض إلى الخزانة العامة للدولة.

مادة 8 - يتولى إدارة الهيئة مجلس إدارة يشكل بقرار من رئيس مجلس الوزراء برئاسة الوزير المختص وعضوية كل من:

(أ) الرئيس التنفيذي للهيئة.

(ب) مستشار من مجلس الدولة يختاره رئيساً مجلس الدولة.

(ج) ممثل لوزارة الدفاع يختاره وزير الدفاع.

(د) ممثل لوزارة الداخلية يختاره وزير الداخلية.

(هـ) ممثل لوزارة المالية يختاره وزير المالية.

(و) ممثل لجهاز رئاسة الجمهورية يختاره رئيس ديوان رئيس الجمهورية.

(ز) ممثل لجهاز المخابرات العامة يختاره رئيس جهاز المخابرات العامة.

(ح) سبعة أعضاء من ذوي الخبرة يختارهم الوزير المختص.

تكون مدة عضوية مجلس الإدارة ثلاث سنوات قابلة للتجديد، ويصدر بتحديد مكافأة العضوية قرار من رئيس مجلس الوزراء.

ولمجلس الإدارة أن يُشكل من بين أعضائه لجنة أو أكثر يعهد إليها بصفة مؤقتة ببعض المهام، وله أن يفوض رئيس مجلس الإدارة أو الرئيس التنفيذي للهيئة في بعض اختصاصاته.

مادة 9 - مجلس إدارة الهيئة هو السلطة المسئولة عن شئونها وتصريف أمورها، ويُباشر اختصاصاته على الوجه المبين في هذا القانون، وله أن يتخذ ما يراه لازماً من قرارات لتحقيق الأغراض التي أُنشئت الهيئة من أجلها، وله على الأخص ما يأتي:

(أ) وضع نظم وقواعد التوقيع الإليكتروني والمعاملات الإليكترونية طبقاً لأحكام القوانين واللوائح المنظمة لها.

(ب) وضع القواعد الفنية والإدارية والمالية والضمانات الخاصة بإصدار التراخيص اللازمة لمزاولة أنشطة خدمات التوقيع الإليكتروني وغيرها من الأنشطة في مجال المعاملات الإليكترونية وتكنولوجيا المعلومات.

(ج) تحديد الخدمات التي تؤديها الهيئة للغير في مجال تكنولوجيا المعلومات والاتصالات، ومقابل أداء هذه الخدمات.

(د) وضع القواعد التي تكفل احترام تقاليد المهنة في مجال المعاملات الإليكترونية وتكنولوجيا المعلومات والاتصالات.

(هـ) وضع اللوائح الداخلية المتعلقة بالشئون الفنية والمالية والإدارية، ولوائح المشتريات والمخازن، وغيرها من اللوائح المتعلقة بتنظيم نشاط الهيئة، وذلك دون التقيد بالقواعد والنظم الحكومية.

(و) اعتماد مشروع الموازنة السنوية للهيئة.

(ز) وضع لائحة شئون العاملين بالهيئة المنظمة لتعيينهم وتحديد رواتبهم وبدلاتهم ومكافآتهم وترقياتهم وتأديبهم وإنهاء خدمتهم وسائر شئونهم الوظيفية، وذلك مع مراعاة قواعد الكفاءة الإنتاجية وتوازن اقتصاديات الهيئة وبالتشاور مع المنظمة النقابية ذات الصلة، ودون التقيد بقواعد ونظم العاملين المدنيين بالدولة.

(ح) وضع خطط وبرامج التدريب والتأهيل على صناعة تكنولوجيا المعلومات.

ويصدر باللوائح والنظم المنصوص عليها في هذه المادة قرار من الوزير المختص.

مادة 10 - يجتمع مجلس الإدارة بدعوة من رئيسه مرة على الأقل كل شهر، وكلما اقتضت الضرورة ذلك، ويكون اجتماعه صحيحاً بحضور أغلبية أعضائه، وتصدر قراراته بأغلبية أصوات الحاضرين وعند التساوي يرجح الجانب الذي منه الرئيس.

وللمجلس أن يدعو لحضور جلساته مَن يرى الاستعانة بخبراتهم دون أن يكون لهم صوت معدود في المداولات.

مادة 11 - للهيئة رئيس تنفيذي يصدر بتعيينه وتحديد معاملته المالية قرار من رئيس مجلس الوزراء بناء على اقتراح الوزير المختص.

ويُمثل الرئيس التنفيذي الهيئة أمام القضاء وفي علاقتها بالغير ويكون مسئولاً أمام مجلس الإدارة عن سير أعمال الهيئة فنياً وإدارياً ومالياً، ويختص بما يأتي:

(أ) تنفيذ قرارات مجلس الإدارة.

(ب) إدارة الهيئة وتصريف شئونها والإشراف على سير العمل بها.

(ج) عرض تقارير دورية على مجلس الإدارة عن نشاط الهيئة وسير العمل بها، وما تم إنجازه وفقاً للخطط والبرامج الموضوعة، وتحديد معوّقات الأداء، والحلول المقترحة لتفاديها.

(د) القيام بأية أعمال أو مهام يكلفه بها مجلس الإدارة.

(هـ) الاختصاصات الأخرى التي تُحددها اللوائح الداخلية للهيئة.

المحرر، - يحل الرئيس التنفيذي محل رئيس مجلس إدارة الهيئة حال غيابه

مادة 13 - تلتزم جميع الجهات والشركات العاملة في مجال المعاملات الإليكترونية وتكنولوجيا المعلومات بموافاة الهيئة بما تطلبه من تقارير أو إحصاءات أو معلومات تتصل بنشاط الهيئة.

مادة 14 - للتوقيع الإليكتروني، في نطاق المعاملات المدنية والتجارية والإدارية، ذات الحجية المقررة للتوقيعات في أحكام قانون الإثبات في المواد المدنية والتجارية، إذا روعي في إنشائه وإتمامه الشروط المنصوص عليها في هذا القانون والضوابط الفنية والتقنية التي تُحددها اللائحة التنفيذية لهذا القانون.

مادة 15 - للكتابة الإليكترونية وللمحررات الإليكترونية، في نطاق المعاملات المدنية والتجارية والإدارية، ذات الحجية المقررة للكتابة والمحررات الرسمية والعرفية في أحكام قانون الإثبات في المواد المدنية والتجارية، متى استوفت الشروط المنصوص عليها في هذا القانون وفقاً للضوابط الفنية والتقنية التي تُحددها اللائحة التنفيذية لهذا القانون.

مادة 16 - الصورة المنسوخة على الورق من المحرر الإليكتروني الرسمي حجة على الكافة بالقدر الذي تكون فيها مطابقة لأصل هذا المحرر، وذلك مادام المحرر الإليكتروني الرسمي والتوقيع الإليكتروني موجودين على الدعامة الإليكترونية.

مادة 17 - تسري في شأن إثبات صحة المحررات الإليكترونية الرسمية والعرفية والتوقيع الإليكتروني، فيما لم يرد بشأنه نص في هذا القانون أو في لائحته التنفيذية الأحكام المنصوص عليها في قانون المرافعات المدنية والتجارية.

مادة 18 - يتمتع التوقيع الإليكتروني والكتابة الإليكترونية والمحررات الإليكترونية بالحجية في الإثبات إذا ما توافرت فيها الشروط الآتية:

(أ) ارتباط التوقيع بالموقّع وحده دون غيره.

(ب) سيطرة الموقّع وحده دون غيره على الوسيط الإليكتروني.

(ج) إمكانية كشف أي تعديل أو تبديل في بيانات المحرر الإليكتروني أو التوقيع الإليكتروني.

وتُحدد اللائحة التنفيذية لهذا القانون الضوابط الفنية والتقنية اللازمة لذلك.

مادة 19 - لا تجوز مزاولة نشاط إصدار شهادات التصديق الإليكتروني إلا بترخيص من الهيئة، وذلك نظير مقابل يُحدده مجلس إدارتها وفقاً للإجراءات والقواعد والضمانات التي تُقررها اللائحة التنفيذية لهذا القانون ودون التقيد بأحكام القانون رقم 129 لسنة 1947م بالتزامات المرافق العامة، مع مراعاة ما يأتي:

(أ) أن يتم اختيار المرخص له في إطار من المنافسة والعلانية.

(ب) أن يُحدد مجلس إدارة الهيئة مدة الترخيص بحيث لا تزيد على تسعة وتسعين عاماً.

(ج) أن تحدد وسائل الإشراف والمتابعة الفنية والمالية التي تكفل حسن سير المرفق بانتظام واطّراد.

ولا يجوز التوقف عن مزاولة النشاط المرخص به أو الاندماج في جهة

أخرى، أو التنازل عن الترخيص للغير إلا بعد الحصول على موافقة كتابية مسبقة من الهيئة.

مادة 20 - تُحدد اللائحة التنفيذية لهذا القانون البيانات التي يجب أن تشتمل عليها شهادة التصديق الإليكتروني.

مادة21 - بيانات التوقيع الإليكتروني والوسائط الإليكترونية والمعلومات التي تقدم إلى الجهة المرخص لها بإصدار شهادات التصديق الإليكتروني سرية، ولا يجوز لمن قدمت إليه أو اتصل بها بحكم عمله إفشاؤها للغير أو استخدامها في غير الغرض الذي قدمت من أجله.

مادة 22 - تختص الهيئة باعتماد الجهات الأجنبية المختصة بإصدار شهادات التصديق الإليكتروني، وذلك نظير المقابل الذي يُحدده مجلس إدارة الهيئة، وفي هذه الحالة تكون الشهادات التي تصدرها تلك الجهات ذات الحجية في الإثبات المقررة لما تصدره نظيراتها في الداخل من شهادات نظيرة، وذلك كله وفقاً للقواعد والإجراءات والضمانات التي تُقرها اللائحة التنفيذية لهذا القانون.

مادة 23 - مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يُعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من:

(أ) أصدر شهادة تصديق إليكتروني دون الحصول على ترخيص بمزاولة النشاط من الهيئة.

(ب) أتلف أو عيّب توقيعاً، أو وسيطاً، أو محرراً إليكترونياً، أو زوّر شيئاً من ذلك بطريق الاصطناع، أو التعديل، أو التحوير، أو بأي طريق آخر.

(ج) استعمل توقيعاً، أو وسيطاً، أو محرراً إليكترونياً معيباً أو مزوراً مع علمه بذلك.

(د) خالف أياً من أحكام المادتين (19)، (21) من هذا القانون.

(هـ) توصّل بأية وسيلة إلى الحصول بغير حق على توقيع، أو وسيط أو محرر إليكتروني، أو اخترق هذا الوسيط، أو اعترضه، أو عطله عن أداء وظيفته.

وتكون العقوبة على مخالفة المادة (13) من هذا القانون، الغرامة التي لا تقل عن خمسة آلاف جنيه ولا تجاوز خمسين ألف جنيه.

وفي حالة العود تزاد بمقدار المثل المقررة ؛ العقوبة المقررة لهذه الانتشار، حديها الأدنى والأقصى.

وفي جميع الأحوال يحكم نشر حكم الإدانة في جريدتين يوميتين واسعتي الانتشار، وعلى شبكات المعلومات الإليكترونية المفتوحة على نفقة المحكوم عليه.

مادة 24 - يُعاقب المسئول عن الإدارة الفعلية للشخص الاعتباري المخالف بذات العقوبات المقررة عن الأفعال التي تُرتكب بالمخالفة لأحكام هذا القانون، إذا كان إخلاله بالواجبات التي تفرضها عليه تلك الإدارة قد أسهم في وقوع الجريمة مع علمه بذلك.

ويكون الشخص الاعتباري مسئولاً بالتضامن عن الوفاء بما يحكم به من عقوبات مالية وتعويضات، إذا كانت المخالفة قد ارتُكبت من أحد العاملين به باسم ولصالح الشخص الاعتباري.

مادة 25 - يكون للعاملين بالهيئة الذين يصدر بهم قرار من وزير العدل بالاتفاق مع الوزير المختص صفة مأموري الضبط القضائي بالنسبة إلى الجرائم التي تقع في حدود اختصاصهم بالمخالفة لأحكام هذا القانون.

مادة 26 - مع عدم الإخلال بأحكام المادة (23) من هذا القانون، يكون للهيئة، إذا خالف المرخص له بإصدار شهادات تصديق إليكتروني شروط

الترخيص أو خالف أياً من أحكام المادة (19) من هذا القانون، أن تلغي الترخيص، كما يكون لها أن توقف سريانه حتى إزالة أسباب المخالفة، وذلك كله وفقاً للقواعد والإجراءات التي تُحددها اللائحة التنفيذية لهذا القانون.

مادة 27 - على كل مَن يُباشر نشاط إصدار شهادات التصديق الإليكتروني قبل تاريخ العمل بهذا القانون أن يوفق أوضاعه طبقاً لأحكامه خلال مدة لا تجاوز ستة أشهر من تاريخ صدور لائحته التنفيذية، وذلك وفقاً للقواعد والإجراءات التي تنص عليها هذه اللائحة.

مادة 28 - لا تسري أحكام المادة (13) من هذا القانون على أجهزة رئاسة الجمهورية ،والقوات المسلحة، ووزارة الداخلية، وجهاز المخابرات العامة، وهيئة الرقابة الإدارية.

مادة 29 - يصدر الوزير المختص اللائحة التنفيذية لهذا القانون خلال ستة أشهر من تاريخ نشره.

مادة 30 - ينشر هذا القانون في الجريدة الرسمية، ويعمل به اعتباراً من اليوم التالي لتاريخ نشره.

يبصم هذا القانون بخاتم الدولة، وينفذ كقانون من قوانينها. صدر برئاسة الجمهورية في غرة ربيع الأول سنة 1425 هـ (الموافق 21 أبريل سنة 2004 م).

الملحق رقم (2)

نظام مكافحة جرائم المعلوماتية، الصادر بالمرسوم الملكي رقم 17 بتاريخ 1428/3/8

المادة الأولى - يُقصد بالألفاظ والعبارات الآتية - أينما وردت في هذا النظام - المعاني المبينة أمامها ما لم يقتضِ السياق خلاف ذلك:

1 - الشخص: أي شخص ذي صفة طبيعية أو اعتبارية، عامة أو خاصة.

2 - النظام المعلوماتي، مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها، وتشمل الحاسبات الآلية.

3 - الشبكة المعلوماتية: ارتباط بين أكثر من حاسب آلي أو نظام معلوماتي للحصول على البيانات وتبادلها، مثل الشبكات الخاصة والعامة والشبكة العالمية (الانترنت).

4 - البيانات: المعلومات، أو الأوامر، أو الرسائل، أو الأصوات، أو الصور التي تُعد، أو التي سبق إعدادها، لاستخدامها في الحاسب الآلي، وكل ما يمكن تخزينه، ومعالجته، ونقله، وإنشاؤه بوساطة الحاسب الآلي، كالأرقام والحروف والرموز وغيرها.

5 - برامج الحاسب الآلي: مجموعة من الأوامر والبيانات التي تتضمن توجيهات أو تطبيقات حين تشغيلها في الحاسب الآلي، أو شبكات الحاسب الآلي، وتقوم بأداء الوظيفة المطلوبة.

6 - الحاسب الآلي: أي جهاز إليكتروني ثابت أو منقول سلكي أو لاسلكي يحتوي على نظام معالجة البيانات، أو تخزينها، أو إرسالها، أو استقبالها، أو تصفحها، يؤدي وظائف محددة بحسب

البرامج، والأوامر المعطاة له.

7 - الدخول غير المشروع، دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع إليكتروني، أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرَّح لذلك الشخص بالدخول إليها.

8 - الجريمة المعلوماتية: أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام.

9 - الموقع الإليكتروني: مكان إتاحة البيانات على الشبكة المعلوماتية من خلال عنوان محدد.

10 - الالتقاط: مشاهدة البيانات، أو الحصول عليها دون مسوِّغ نظامي صحيح.

المادة الثانية - يهدف هذا النظام إلى الحد من وقوع جرائم المعلوماتية، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها، وبما يؤدي إلى ما يأتي:

1 - المساعدة على تحقيق الأمن المعلوماتي.

2 - حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية.

3 - حماية المصلحة العامة، والأخلاق، والآداب العامة.

4 - حماية الاقتصاد الوطني.

المادة الثالثة - يُعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

1 - التصنت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد

أجهزة الحاسب الآلي - دون مسوّغ نظامي صحيح - أو التقاطه أو اعتراضه.

2 - الدخول غير المشروع لتهديد شخص أو ابتزازه؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعاً.

3 - الدخول غير المشروع إلى موقع إليكتروني، أو الدخول إلى موقع إليكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه.

4 - المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها.

5 - التشهير بالآخرين، وإلحاق الضرر بهم، عبر وسائل تقنيات المعلومات المختلفة.

المادة الرابعة - يُعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

1 - الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة.

2 - الوصول - دون مسوّغ نظامي صحيح - إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تُتيحه من خدمات.

المادة الخامسة - يُعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب

أياً من الجرائم المعلوماتية الآتية:

1 - الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها.

2 - إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها أو تدميرها، أو مسح البرامج، أو البيانات الموجودة، أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها.

3 - إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت.

المادة السادسة - يُعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

1 - إنتاج ما من شأنه المساس بالنظام العام، أو القيم الدينية، أو الآداب العامة، وحرمة الحياة الخاصة، أو إعداده، أو إرساله، أو تخزينه عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي.

2 - إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، للاتجار في الجنس البشري، أو تسهيل التعامل به.

3 - إنشاء المواد والبيانات المتعلقة بالشبكة الإباحية، أو أنشطة الميسر المخلة بالآداب العامة، أو نشرها، أو ترويجها.

4 - إنشاء موقع على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي أو نشره، للإتجار بالمخدرات، أو المؤثرات العقلية، أو ترويجها، أو طرق تعاطيها، أو تسهيل التعامل بها.

المادة السابعة - يُعاقب بالسجن مدة لا تزيد على عشر سنوات وبغرامة لا تزيد على خمسة ملايين ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أياً من الجرائم المعلوماتية الآتية:

1 - إنشاء موقع لمنظمات إرهابية على الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي، أو نشره لتسهيل الاتصال بقيادات تلك المنظمات، أو أي من أعضائها، أو ترويج أفكارها، أو تمويلها، أو نشر كيفية تصنيع الأجهزة الحارقة، أو المتفجرات، أو أداة تستخدم في الأعمال الإرهابية.

2 - الدخول غير المشروع إلى موقع إليكتروني، أو نظام معلوماتي مباشرةً، أو عن طريق الشبكة المعلوماتية، أو أحد أجهزة الحاسب الآلي للحصول على بيانات تمس الأمن الداخلي أو الخارجي للدولة، أو اقتصادها الوطني.

المادة الثامنة - لا تقل عقوبة السجن أو الغرامة عن نصف حدها الأعلى إذا اقترنت الجريمة بأي من الحالات الآتية:

1 - ارتكاب الجاني الجريمة من خلال عصابة منظمة.

2 - شغل الجاني وظيفة عامة، واتصال الجريمة بهذه الوظيفة، أو ارتكابه الجريمة مستغلاً سلطاته أو نفوذه.

3 - التغرير بالقصر ومن في حكمهم، واستغلالهم.

4 - صدور أحكام محلية أو أجنبية سابقة بالإدانة بحق الجاني في جرائم مماثلة.

المادة التاسعة - يُعاقب كل من حرَّض غيره، أو ساعده، أو اتفق معه على ارتكاب أي من الجرائم المنصوص عليها في هذا النظام؛ إذا وقعت الجريمة بناء على هذا التحريض، أو المساعدة، أو الاتفاق، بما لا يتجاوز الحد الأعلى للعقوبة المقررة لها، ويُعاقب بما لا يتجاوز نصف الحد الأعلى للعقوبة

المقررة لها إذا لم تقع الجريمة الأصلية.

المادة العاشرة - يُعاقب كلُّ مَن شرع في القيام بأي من الجرائم المنصوص عليها في هذا النظام بما لا يتجاوز نصف الحد الأعلى للعقوبة المقررة.

المادة الحادية عشرة - للمحكمة المختصة أن تعفي من هذه العقوبات كل مَن يُبادر من الجناة بإبلاغ السلطة المختصة بالجريمة قبل العلم بها وقبل وقوع الضرر، وإن كان الإبلاغ بعد العلم بالجريمة تعين للإعفاء أن يكون من شأن الإبلاغ ضبط باقي الجناة في حال تعددهم، أو الأدوات المستخدمة في الجريمة.

المادة الثانية عشرة - لا يخل تطبيق هذا النظام بالأحكام الواردة في الأنظمة ذات العلاقة وخاصة بما يتعلق بحقوق الملكية الفكرية، والاتفاقيات الدولية ذات الصلة التي تكون المملكة طرفاً فيها.

المادة الثالثة عشرة - مع عدم الإخلال بحقوق حسني النية، يجوز الحكم بمصادرة الأجهزة، أو البرامج، أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا النظام، أو الأموال المحصلة منها. كما يجوز الحكم بإغلاق الموقع الإليكتروني، أو مكان تقديم الخدمة إغلاقاً نهائياً أو مؤقتاً متى كان مصدراً لارتكاب أي من هذه الجرائم، وكانت الجريمة قد ارتكبت بعلم مالكه.

المادة الرابعة عشرة - تتولى هيئة الاتصالات وتقنية المعلومات وفقاً لاختصاصها تقديم الدعم والمساندة الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة.

المادة الخامسة عشرة - تتولى هيئة التحقيق والادعاء العام التحقيق والادعاء في الجرائم الواردة في هذا النظام.

المادة السادسة عشرة - ينشر هذا النظام في الجريدة الرسمية ويُعمل به بعد (مائة وعشرين) يوماً من تاريخ نشره.

المراجع

(أ) المراجع العربية:

1 - حسني، محمود نجيب، شرح قانون العقوبات، القسم العام، الطبعة السادسة، دار النهضة العربية، القاهرة، 1989م.

2 - حسني، محمود نجيب، شرح قانون العقوبات، القسم الخاص، الجرائم المضرة بالمصلحة العامة، دار النهضة العربية، القاهرة 1972م.

3 - حسنى، محمود نجيب، شرح قانون الإجراءات الجنائية، الطبعة الثالثة، دار النهضة العربية، القاهرة.

4 - سلامة، مأمون، الإجراءات الجنائية في القانون المصري، ج 2، ط2000م، دار النهضة العربية، مصر.

5 - سلامة، مأمون، الإجراءات الجنائية في التشريع الليبي، ج 2، ط2000، منشورات المكتبة الجامعة، القاهرة.

6 - عبد الخالق، حسن، أصول الإجراءات الجنائية، الطبعة الثانية عشر، عام 2005 م، دار الطبي للطباعة والنشر، بالقاهرة.

7 - الشهاوى، قدري عبد الفتاح ضوابط الحبس الاحتياطي، منشأة المعارف، بالإسكندرية، 2003 م.

8 - الزهنى، لأدور غالي، الإجراءت الجنائية، الطبعة الثالثة، مكتبة غريب

بالقاهرة، 1990م.

9 - ظفير، سعد بن محمد، الإجراءات الجنائية في المملكة السعودية، الرياض طبعه 1424هـ.

10 - عثمان، آمال عبد الرحيم، الإثبات الجنائي ووسائل التحقيق العلمية، دار النهضة العربية، القاهرة، 1975م.

11 - تاج الدين، مدني عبد الرحمن، أصول التحقيق الجنائي وتطبيقاتها في المملكة ص286، الرياض معهد الإدارة 1425هـ.

12 - مصطفى، محمود محمود، شرح قانون الإجراءات الجنائية، ط11، القاهرة، 1976م.

13 - النجار، عماد عبد الحميد، الادعاء العام والمحاكمة الجنائية وتطبيقاتها في المملكة العربية السعودية، الرياض، طبعة 1417.

14 - الشوا، محمد دراسة، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة 1994م.

15 - مغايرة، منصور دراسة، حول «الجرائم المعلوماتية»، مكتبة جامعة الحكمة، 1999م - 2000م.

16 - هلال، محمد رضوان، المحكمة الرقمية، دار العلوم للنشر والتوزيع، القاهرة 2007م.

17 - الألفي، محمد محمد، (2007 م)، مؤتمر الحكومة الإليكترونية السادس «الإدارة العامة الجديدة والحكومة الإليكترونية» دبي، دولة الإمارات العربية المتحدة9 - 12ديسمبر 2007 م، ورقه عن المحكمة الإليكترونية بين الواقع والمأمول.

18 - الجنيدي، ماهر (أ). (1999م). النصر للأقوى والأذكى والقذر، مجلة انترنت العالم العربي، (نوفمبر)،

19 - ممدوح، خالد فن التحقيق الجنائي في الجرائم الإليكترونية، دار الفكر الجامعي، 2009م.

20 - إبراهيم، خالد ممدوح الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2009.

21 - إبراهيم، خالد ممدوح الجرائم المعلوماتية، الدليل الإليكتروني في الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2007.

22 - إبراهيم، خالد ممدوح الجرائم المعلوماتية، أمن الجريمة الإليكترونية، دار الفكر الجامعي، الإسكندرية، 2008.

23 - خميس، فوزي، جرائم المعلوماتية وحماية الملكية المعلوماتية وبنوك وقواعد المعلومات، محاضرة ألقيت في نقابة المحامين في بيروت بتاريخ 1999/2/25م.

24 - عوض، فوزي رياض، مشروعية الدليل الجنائي في مرحلة المحاكمة وما قبلها، دراسة تحليلية تأصيلي مقارنة، دار النهضة العربية - القاهرة - 1997م.

25 - البحر، ممدوح خليل، أصول المحاكمات الجزائية، ط1، دار الثقافة، عمان، 1998م.

26 - حجازي، عبد الفتاح بيومي، الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت، دار الكتب القانونية، القاهرة 2002م.

27 - حجازي، عبد الفتاح بيومي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، دار الكتب القانونية، القاهرة، 2002م.

28 - علي، حجازي عبد الفتاح، جرائم الكمبيوتر والانترنت، دار الكتب القانونية، القاهرة، 2005م.

29 - بيومي، حجازي عبد الفتاح، صراع الكمبيوتر والانترنت، في القانون العربي النموذجي، دار الكتب القانونية، القاهرة، 2007م.

30 - علي، عبد الصبور عبد القوي، الجريمة الإليكترونية، دار العلوم للنشر والتوزيع، القاهرة 2007م.

31 - علي، عبدا لصبور عبدا لقوي، التجارة الإليكترونية والقانون، دار العلوم للنشر والتوزيع، القاهرة 2007م.

32 - حسن، عبد الصبور عبد القوي، التنظيم القانوني التجارة الإليكترونية، مكتبة القانون والاقتصاد، الرياض 2011م.

33 - حسن، سعيد عبد اللطيف، الإثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، الجرائم الواقعة في مجال تكنولوجيا المعلومات، ط1، دار النهضة العربية، القاهرة، 1999م.

34 - رستم، هشام محمد فريد، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، 1994م.

35 - رستم، هشام محمد فريد، قانون العقوبات ومخاطر تقنية المعلومات، الطبعة الأولى، مكتبة الآلات الحديثة، اسيوط، 1992.

36 - رستم، هشام محمد فريد، الجرائم المعلوماتية (أصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي) بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت كلية الشريعة والقانون، بجامعة الإمارات العربية المتحدة، عام 2000م.

37 - الطوالبه، على حسن، مشروعية الدليل الإليكتروني المستمد من التفتيش الجنائي، «دراسة مقارنة الحقوق جامعة العلوم التطبيقية»، البحرين، 2005م.

38 - الطوالبه، على حسن، التفتيش الجنائي على نظم الحاسوب والانترنت - دراسة مقارنة، ط1، عالم الكتب الحديث، اربد، 2004م.

39 - الكركي، كمال، جرائم الحاسوب ودور مديرية الأمن في مكافحتها، ورقة عمل مقدمة إلى ندوة قانون حماية حق المؤلف، نظرة إلى المستقبل، المنعقدة في عمان بتاريخ 1999/7/5م.

40 - أبو علي، نزار فايز، فيروسات الكمبيوتر، دار حنين للنشر، عمان 1994م.

41 – المناعسة، أسامة أحمد، والزعبي جلال محمد، الهواوشة، وصايل، جرائم الحاسب الآلي والانترنت، دراسة تحليلية مقارنة، ط1، دار وائل، عمان، 2001م.

42 – عيسى، طوني، التنظيم القانوني لشبكة الانترنت، منشورات صادر الحقوقية، 2001م.

43 – الصغير، جميل عبد الباقي، الانترنت والقانون الجنائي، دار النهضة العربية، 1992م.

44 – الصغير، جميل عبد الباقي، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، (أجهزة الرادار – الحاسبات الآلية – البصمة الوراثية)، دراسة مقارنة، دار النهضة العربية، القاهرة، 2001م.

45 – الصغير، جميل عبد الباقي، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، الطبعة الأولى، منشورات دار النهضة العربية، القاهرة، 1992م.

46 – شتا، محمد محمد، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، 2001م.

47 – العكيلي، عبد الأمير، أصول الإجراءات الجنائية في قانون أصول المحاكمات الجزائية، ج1، ط1، مطبعة المعارف، بغداد، 1975م.

48 – شرف الدين، احمد، حجية الرسائل الإليكترونية في الإثبات، شبكة المعلومات القانونية العربية، East Law. com - 2007.

49 – صالح، نائل عبد الرحمن، محاضرات في قانون أصول المحاكمات الجزائية، ط1، دار الفكر العربي، عمان، 1997م.

50 – البداينة، ذياب. (1999م). الاجتماعية للانترنت، ورقة قدمت في الدورة التدريبية حول شبكة الانترنت من منظور أمني، أكاديمية نايف العربية للعلوم الأمنية، بيروت، لبنان.

51 – البداينة، ذياب. (1420هـ). جرائم الحاسب والانترنت، أبحاث الندوة

العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية، تونس، تونس (93-124).

52 - عفيفي، عفيفي كامل، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، 2003.

53 - عوض، أحمد عوض، قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائية المقارنة، دار النهضة العربية، القاهرة، 1994م.

54 - عوض، محمد محيي الدين، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)، ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي، المنعقد بالقاهرة في الفترة من -25 28 أكتوبر 1993م.

55 - أحمد، هلالي عبد اللاه، التزام الشاهد بالإعلام في الجرائم المعلوماتية، دراسة مقارنة، النسر الذهبي، القاهرة، 2000م.

56 - أحمد، هلالي عبد اللاه، حجية المخرجات الكمبيوترية في الإثبات الجنائي، ط1، دار النهضة العربية، القاهرة، 1997م.

57 - أحمد، هلالي عبد اللاه، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دراسة مقارنة، ط1، دار النهضة العربية، القاهرة، 1997م.

58 - أحمد، هلالي عبد اللاه، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية (على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001م)، الطبعة الأولى، دار النهضة العربية القاهرة، 2006م.

59 - البشري، عبد الله عبد العزيز. (1420هـ). التقنية والجرائم المستحدثة، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية، تونس، تونس (195 - 233).

60 – طلبة، محمد فهمي وآخرون، دائرة المعارف الحاسب الإليكتروني، مجموعة كتب دلتا، مطابع المكتب المصري الحديث، القاهرة، 1991م.

61 – البشري، محمد الأمين، الأدلة الجنائية الرقمية، مفهومها ودورها في الإثبات، المجلة العربية للدراسات الأمنية والتدريب، المجلد 17، العدد 33، السنة 17، الرياض، أبريل 2002م.

62 – جيتس وآخرون، بيل، المعلوماتية بعد الانترنت (طريق المستقبل)، ترجمة رضوان، عبد السلام، سلسلة عالم المعرفة، المجلس الوطني للثقافة والفنون الآداب، العدد 231، الكويت، مارس 1988م.

63 – عابد، عبد الحافظ عبد الهادي، الإثبات الجنائي بالقرائن، دراسة مقارنة، دار النهضة العربية، القاهرة 1998م.

64 – تمام، أحمد حسام طه، الجرائم الناشئة عن استخدام الحاسوب، (الحماية للحاسوب)، دراسة مقارنة، دار النهضة، القاهرة 2000م.

65 – الأمين، محمد، العدالة الجنائية ومنع الجريمة، دراسة مقارنة، ط1، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 1997م.

66 – محمد، عادل ريان. (1995م)، جرائم الحاسب الآلي وأمن البيانات، العربي، (440)، 73 – 77.

67 – بوحويش، عطية عثمان محمد، حجية الدليل الرقمي في إثبات جرائم المعلوماتية، رسالة التخصص العالي (الماجستير)، مقدمة إلى أكاديمية الدراسات العليا/فرع بنغازي، للعام الجامعي 2009م.

68 – عقيدة، محمود أبو العلا، شرح قانون الإجراءات الجنائية، الأردن، دار الحكمة، ط 2001م.

69 – مندور، محمد محمود، الجرائم الحاسب الآلية، دورة فيروس الحاسب الآلي، مكتب الأفاق المتحدة: الرياض، 1410هـ.

70 – السعيد، كامل، شرح الأحكام العامة في قانون العقوبات الأردني والقانون المقارن، الطبعة الثانية، دار الفكر للنشر والتوزيع، عمان،

1983م.

71 - قشقوش، هدى، جرائم الحاسب الإليكتروني في التشريع المقارن، الطبعة الأولى دار النهضة العربية، القاهرة، 1992م.

72 - منصور، محمد حسن، المسؤولية الإليكترونية، دار الجامعة للنشر، الإسكندرية، 2003م.

73 - حسين، مدحت، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، القاهرة، 2000م.

74 - حسين، محمد عبد الظاهر، المسئولية القانونية في مجال شبكات الانترنت، دار النهضة العربية، القاهرة 2002م.

75 - الشاذلي، فتوح، القانون الدولي الجنائي، دار المطبوعات الجامعية، الإسكندرية، 2001م.

76 - سرور، أحمد فتحي، الوسيط في الاجراءات الجنائية، دار النهضة العربية، القاهرة 1985م.

77 - الشريف، عمر واصف، النظرية العامة في التوقيف الاحتياطي، الطبعة الأولى، منشورات الحلبي الحقوقية، ببيروت، 2004م.

78 - اللحيدان، فهد بن عبد الله، الانترنت، شبكة المعلومات العالمية، الطبعة الأولى، الناشر غير معروف، 1996م.

79 - المرصفاوي، حسن صادق، قانون العقوبات الخاص، منشأة المعارف، الإسكندرية، مصر 1991م.

80 - الفيومي محمد، مقدمة في علم الحاسبات الإليكترونية والبرمجة بلغة بيسك»، دار الفرقان، 1984م.

81 - مصلح، يحيى، التجارة على الانترنت. سايمون كيونس، له إلى العربية، بيت الأفكار الدولية بأمريكا 1999م.

82 - عبادة، عبادة أحمد، التدمير المتعمد لأنظمة المعلومات الإليكترونية

مركز البحوث والدراسات، شرطة دبي بدولة الإمارات العربية المتحدة2005م

83 - الطويل، خالد بن محمد، التعامل مع الاعتداءات الإليكترونية من الناحية الأمنية مركز المعلومات الوطني، وزارة الداخلية، ورقة عمل مقدمة لورشة العمل الثالثة (أحكام في المعلوماتية) الذي نظمه مشروع الخطة الوطنية لتقنية المعلومات 19 10 1423هـ الرياض.

84 - عرب، يونس، قانون الكمبيوتر، موسوعة القانون وتقنية المعلومات، منشورات اتحاد المصارف العربية، الطبعة الأولى، الجزء الأول، 2001م.

85 - عرب، يونس، جرائم الكمبيوتر والانترنت، المركز العربي للدراسات والبحوث الجنائية، أبو ظبي 10-2002/2/12م.

86 - عرب، يونس، صور الجرائم الإليكترونية واتجاهاتها تبويبها ورقة عمل سنة 2006م.

87 - عرب، يونس، جرائم الكمبيوتر والانترنت، موسوعة القانون وتقنية المعلومات، منشورات اتحاد المصارف العربية، الطبعة الأولى، الجزء الثاني، 2002م.

88 - عرب، يونس، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والانترنت، الجزء الأول، منشورات إتحاد المصارف العربية، الطبعة الأولى 2000م.

89 - الخليل، عماد علي، التكييف القانوني لإساءة استخدام أرقام البطاقات عبر شبكة الانترنت، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، الذي نظمته كلية الشريعة والقانون، بجامعة الإمارات العربية المتحدة، عام2000م.

90 - الجنبيهي، منير، والجنبيهي، ممدوح البنوك الإليكترونية ط 2، 2006م، دار الفكر الجامعي، الإسكندرية

91 - الجنبيهي، منير، والجنبيهي، ممدوح، صراخ الانترنت وسائل مكافحتها،

2005م، دار الفكر الجامعي، الإسكندرية.

92 - سلامة، محمد عبد الله أبو بكر، جرائم الكومبيوتر والانترنت موسوعة جرائم المعلوماتية، منشأة المعارف، الإسكندرية، 2006م.

93 - الشافعي، محمد إبراهيم محمد، النقود الإليكترونية، مجلة الأمن والحياة، أكاديمية الشرطة، دبي، س 12، ع1، يناير، 2004م.

94 - مراد، عبد الفتاح، شرح التحقيق الجنائي الفني والبحث الجنائي، دار الكتب والوثائق المصرية، القاهرة 2000م.

95 - عمر، ممدوح خليل، حماية الحياة الخاصة والقانون الجنائي، دار النهضة العربية، القاهرة 1983م.

96 - قايد، أسامة عبد الله، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، 1994م.

97 - عبد المطلب، ممدوح عبد الحميد، جرائم استخدام شبكة المعلومات العالمية (الجريمة عبر الانترنت)، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، بجامعة الإمارات العربية المتحدة، عام 2000م.

98 - القاسم، محمد بن عبد الله، والزهراني، رشيد، والسند، عبد الرحمن بن عبد الله، العمري، عاطف، تجارب الدول في مجال أحكام في المعلوماتية، مشروع الخطة الوطنية لتقنية المعلومات، 1423هـ.

99 - حجازي، سهير، التهديدات الإجرامية للتجارة الإليكترونية، مركز البحوث والدراسات، شرطة دبي بدولة الإمارات العربية المتحدة، 2005م.

100 - طه، محمود سري، الكمبيوتر في مجالات الحياة، الهيئة المصرية العامة للكتاب، القاهرة، 1990م.

101 - صدق، عبد الرحيم، الإرهاب السياسي والقانون الجنائي، دار النهضة العربية، القاهرة، 1985م.

102 - لويس، بدر سمحمد،، أثر التطور التكنولوجي مع الحريات الشخصية في النظم السياسية، رسالة الدكتوراه، حقوق القاهرة 1982م.

103 - سفر، حسن بن محمد، الإرهاب والعنف في ميزان الشريعة الإسلامية والقانون الدولي، بحث مقدم لمجمع الفقه الإسلامي الدولي، الدورة الرابعة عشرة، الدوحة، قطر 2003/1/11م.

104 - عباس، عمرو حسين، أدلة الإثبات الجنائي والجرائم الإليكترونية، جامعة الدول العربية، مصر، سنة 2008م.

105 - غاري، ج. بيتر، ثقافة الحاسوب، الوعي والتطبيق والبرمجة، الطبعة الأولى، ترجمة ونشر مؤسسة الأبحاث اللغوية، نيقوسيا، 1987م.

106 - رون وايت، كيف تعمل الحواسيب، ترجمة ونشر الدار العربية للمعرفة والعلوم، بيروت 1999م.

107 - سلامة، محمد عبد الله أبو بكر، جرائم الكومبيوتر والانترنت موسوعة جرائم المعلوماتية، منشأة المعارف، الاسكندرية 2006.م.

108 - غوشه، عصام. «نظرة إلى عالم الفيروسات»، مجلة الحاسوب، العدد 23، 1995م.

109 - البربري، صالح أحمد، دور الشرطة في مكافحة جرائم الانترنت في إطار الاتفاقية الأوروبية، الموقعة في بودابست في 2001/11/23 - www.arablawinfo.com

110 - الحميد، محمد دباس، وماركوا إبراهيم نينو، حماية أنظمة المعلومات، دار الحامد، الطبعة الأولى، سنة 2007م.

111 - ياسين، صباغ محمد محمد، الجهود الدولية والتشريعية لمكافحة الإرهاب وقرب العالم الجديد، دار الرضوان، القاهرة، 2005م.

(ب) المراجع الأجنبية:

1 - Eoghan Casey, Digital Evidence and Computer Crime, Academic Pres,. 1 st edition, 2000.

2 - David J David, Internet Detective-An Investigator's Guide, Police Research Group, 1998.

3 - Interpol, Computers and Crime, Manual of Standards and Procedures, 1996.

4 - Interpol, Scoping and responding to information Technology crime in Asia-South Pacific Region, 2001.

5 - Tom Douglas Brian Loader, Thomas Douglas, Cyber crime: Law Enforcement, Security, and Surveillance in the Information Age, 1 st edition, Rutledge, 2000.

6 - Donn B. Parker, Fighting Computer Crime: A New Framework for Protecting Information, 1 edition, John Wiley & Sons 1998.

7 - Edward Waltz, Information Warfare Principles and Operations, 1998.

8 - Laura E. Quarantiello, Tiare Publications, Cyber Crime: How to Protect Your-self from Computer Criminals, 1996.

9 - Tom forester, Essential proplems to Hig-Tech Society First MIT Pres edition, Cambridge, Massachusetts, 1989, P. 104

10 - Cybercrime: Law Enforcement, Security, and Surveillance in the Information Age.by Tom Douglas Brian Loader. Thomas Douglas,1st edition,) Routledge, 2000

11 - Digital Evidence and Computer Crime, by Eoghan Casey, 1st edition Academic Pr. 2000.

12 - 'Criminal Profiling: An Introduction to Behavioral Evidence Analysis,by Brent E. Turvey, Diana Tamlyn, Jerry Chisum, 1edition. Academic Press Limited 1999.

13 - Fighting Computer Crime: A New Framework for Protecting Information, by Donn B. Parker, 1 edition, John Wiley & Sons 1998.

14 - Information Warfare Principles and Operations, by Edward Waltz 1998.

15 - Francillon (J.) ; Les crimes informatiques ET d' autres crimes dans dommaine de la technologie informatique, Rev. Int. dr. pen. 1993, p. 291.

16 - Kaspersen (H. W. K): computer crimes and others crimes aganiste information technology in the Netherlands. Rev. Int. dr. pen. 1993, p. 474. spec. p. 502.

17 - Meunier (C.): La loi du 28 Nov. 2000 17- relative a la criminalite informatique. Rev. Dr. pen. Crim. 2002, p. 611.

18 - Mohrenschlager (M): computer crimes and others crimes aganiste information technology in the Germany. Rev. Int. dr. pen. 1993, p. 319,. Spec. p. 349.

19 - Padovo (M.): La douane et la cyber - delinquance. G. P. 1996. Doctr. 1325.

20 - Piragaff (D. K.): Computer crimes and others crimes aganiste information technology in the Canada., report, Rev. int. dr. pen. 1993. p. 201.

21 - Sieber (U.): Les crimes informatiques et d' autres crimes dans le dommaine de la technologie informatique, Rev. int. dr. pen. 1993, p. 53.

22 - Spreutels (J. P.): Les crimes informatiques ET d' autres crimes dans le domaine de la technologie informatique en Belgique, Rev.

Int. dr. pen. 1993. p. 161.

23 - Taylor (R.): Computer crime, «in criminal investigation edited» by Charles Swanson, n. chamelin and L. Territto, Hill, inc. 5edition 1992.

24 - Cyber Crime: How to Protect Yourself from Computer Criminals by Laura E. Quarantiello, Tiare Publications, 1996.

(ج) الجرائد والمجلات:

1 – جريدة عكاظ، الإليكترونية.

2 – صحيفة عكاظ، السعودية.

3 – مجلة الدراسات القانونية، جامعة أسيوط، مصر.

4 – مجلة الأمن والقانون، دبي.

5 – جريدة الرأي الأردنية، الأردن.

6 – المجلة العربية للدراسات الأمنية والتدريب، الرياض، السعودية.

(د) مواقع الإنترنت:

1 - www. masress. com

2 - www. Minshawi. com

3 - www. startimes. com

4 - www. alexalaw. com

5 - www. chawkitabib. info

6 - www. lawjo. net

7 - www. journal. cybrarians. info -

8 - www. alarabiya. net

الفهرس

الصفحة

الصفحة

الصفحة

الصفحة

الصفحة

الصفحة

الصفحة

الصفحة

الصفحة

الصفحة

الصفحة

الصفحة

الصفحة

الصفحة

الصفحة

الصفحة

الصفحة

الصفحة



